Популярные лекции
ПО МАТЕМАТИКЕ

В. А. УСПЕНСКИЙ

ТЕОРЕМА ГЁДЕЛЯ О НЕПОЛНОТЕ



ПОПУЛЯРНЫЕ ЛЕКЦИИ ПО МАТЕМАТИКЕ
ВЫПУСК 57

В. А. УСПЕНСКИЙ

ТЕОРЕМА ГЁДЕЛЯ О НЕПОЛНОТЕ



МОСКВА «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
1982

22.12
У 77
УДК 517.11

Успенский В. А.

У 77 Теорема Гёделя о неполноте. — М.: Наука, 1982. — 112 с. — (Популярные лекции по математике). — 15 к.

Брошюра посвящена одному из наиболее замечательных достижений математической логики — теореме Гёделя о неполноте формальной арифметики. В ней излагается доказательство теоремы Гёделя, опирающееся на теорию алгоритмов. Брошюра рассчитана на школьников старших классов, студентов младших курсов и, вообще, всех интересующихся логическими проблемами математики.

У $\frac{1702020000-021}{053(02)-82}$ 82-81

ББК 22.12
517.8

У $\frac{1702020000-021}{053(02)-82}$ 82-81

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Есть в математике темы, пользующиеся достаточной известностью и в то же время признаваемые традицией слишком сложными (или маловажными) для включения в обязательное обучение: обычай относит их к занятиям факультативным, дополнительным, специальным и т. п. В перечне таких тем есть несколько, остающихся сейчас там исключительно в силу инерции. Одной из них является теорема Гёделя.

Несмотря на то, что очень многие математики (и нематематики) слышали о ней, мало кто из них может объяснить, в чем состоит утверждение теоремы Гёделя и тем более как она доказывается. Вместе с тем результат столь важен, а причины, вызывающие неустранимую неполноту (т. е. невозможность добиться того, чтобы каждое истинное утверждение было доказуемо), столь просты, что теорема Гёделя могла бы излагаться на самых младших курсах. Более того, для понимания доказательства необходимо лишь знакомство с простейшей терминологией теории множеств (словами «множество», «функция», «область определения» и тому подобными) и некоторая привычка к восприятию математических рассуждений, так что оно вполне доступно подготовленному школьнику.

Излагаемый в этой брошюре способ доказательства теоремы Гёделя отличен от способа, предложенного самим Гёделем, и опирается на элементарные понятия теории алгоритмов. Все необходимые сведения из этой теории сообщаются по ходу дела, так что читатель одновременно знакомится с основными фактами теории алгоритмов. Брошюра написана на основе статьи автора в журнале «Успехи математических наук», 1974, том 29, выпуск 1 (175). Естественно, что изменение круга предполагаемых читателей сделало

необходимой ее переработку. В частности, некоторые более специальные вопросы, а также библиографические ссылки на оригинальные публикации исключены, и любознательный читатель может найти их в упомянутой статье автора. Одновременно расширен раздел, посвященный связи между семантической и синтаксической формулировками теоремы о неполноте, а также добавлены приложения, посвященные теореме Тарского о невыразимости понятия истины и обоснованию аксиомы арифметичности.

План брошюры таков. В § 1 формулируется теорема о неполноте и уточняется ее формулировка, в частности вводится центральное для данной брошюры понятие дедуктики. В § 2 излагаются на неформальном уровне начальные понятия теории алгоритмов, и на их основе формулируются первые критерии полноты и неполноты. В § 3 продолжается исследование критериев неполноты. В § 4 описывается язык формальной арифметики, дается точное определение понятия истинности утверждения этого языка и точная формулировка теоремы Гёделя о неполноте для формальной арифметики. В § 5 на основе дальнейшего развития тех представлений об алгоритмах, которые были описаны в § 2, — развития, закрепляемого в виде трех аксиом теории алгоритмов, — завершается доказательство теоремы о неполноте формальной арифметики.

Брошюра снабжена шестью приложениями, написанными несколько более сжато, хотя по-прежнему не предполагающими никаких специальных знаний. В первом из них рассматривается вопрос о связи между наличием истинных недоказуемых утверждений и наличием утверждений, не являющихся ни доказуемыми, ни опровержимыми. Во втором доказывается некоторое усиление теоремы Гёделя — теорема Тарского о невыразимости понятия истины. Третье приложение посвящено обоснованию одной из аксиом теории алгоритмов, сформулированных в § 5, а именно, аксиомы арифметичности. С этой целью вводится некоторый конкретный класс алгоритмов — класс адресных программ — и проверяется арифметичность функций, вычисляемых алгоритмами этого класса. В четвертом приложении развитые в § 2 критерии полноты и неполноты применяются к языкам, связанным с так

называемыми ассоциативными исчислениями. Пятое приложение посвящено первоначальной формулировке теоремы о неполноте, предложенной самим Гёделем. Шестое приложение содержит упражнения к некоторым из предыдущих разделов. Наконец, последнее приложение содержит ответы и указания к упражнениям. Приложения не зависят друг от друга и могут читаться в любом порядке, за исключением приложения В, отдельные места которого требуют знакомства с введенными в приложении Б понятиями.

Если после чтения этой брошюры у читателя возникнет желание более близко познакомиться с математической логикой и теорией алгоритмов, он может обратиться к следующим книгам:

1. Машины Тьюринга и рекурсивные функции./Эббинхауз Г.-Д., Якобс К., Ман Ф.-К., Хермес Г. — М.: Мир, 1972, 264 с. (Современная математика. Популярная серия.)
2. Ершов Ю. Л., Палютин Е. А. Математическая логика. — М.: Наука, 1979, 320 с.
3. Клини С. К. Введение в метаматематику. — М.: ИЛ, 1957, 526 с.
4. Клини С. К. Математическая логика. — М.: Мир, 1973, 480 с.
5. Коэн П. Дж. Теория множеств и континуум-гипотеза. — М.: Мир, 1969. Глава 1. Основы математической логики, с. 13—86.
6. Лавров И. А., Максимова Л. Л. Задачи по теории множеств, математической логике и теории алгоритмов. — М.: Наука, 1975, 240 с.
7. Линдон Р. Заметки по логике. — М.: Мир, 1968, 128 с. (Современная математика. Популярная серия.)
8. Мальцев А. И. Алгоритмы и рекурсивные функции. — М.: Наука, 1965, 391 с.
9. Манин Ю. И. Доказуемое и недоказуемое. — М.: Советское радио, 1979, 167 с.
10. Манин Ю. И. Вычислимое и невычислимое. — М.: Советское радио, 1980, 128 с.
11. Мендельсон Э. Введение в математическую логику. — 2-е издание. — М.: Наука, 1976, 320 с.
12. Новиков П. С. Элементы математической логики. — 2-е издание, исправленное. — М.: Наука, 1973, 399 с.
13. Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. — М.: Мир, 1972, 624 с.
14. Фрейденталь Х. Язык логики. — М.: Наука, 1969, 135 с.

§ 1. ПОСТАНОВКА ЗАДАЧИ

Формулировка теоремы о неполноте, которую мы будем уточнять и доказывать, такова: при определенных условиях

в языке существует недоказуемое истинное утверждение.

В этой формулировке едва ли не каждое слово нуждается в разъяснениях. Сделаем такие разъяснения.

1. **Язык.** Мы не будем давать какое бы то ни было определение языка (поскольку не беремся это сделать с достаточной общностью), а ограничимся теми относящимися к языку понятиями, которые единственно и будут нужны нам для дальнейшего. Таких понятий нам потребуется два: «алфавит языка» и «множество истинных утверждений языка».

1.1. Алфавит. Под *алфавитом* понимается конечный список элементарных (т. е. считающихся не членимыми далее) знаков, называемых *буквами* этого алфавита. Конечная цепочка следующих друг за другом букв некоторого алфавита называется *словом* в этом алфавите. Так, слова русского языка (включая и собственные имена) суть слова в 66-буквенном алфавите (33 строчные буквы, 31 прописная буква[1]), дефис, апостроф); десятичные записи натуральных чисел — слова в десятибуквенном алфавите {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}. Для называния алфавитов используются обычно прописные русские буквы. Множество всех слов в алфавите Б будем обозначать $Б^{\infty}$. Предполагается, что для каждого языка имеется такой алфавит, что все выражения этого языка (т. е. имена тех или

[1]) Кроме твердого и мягкого знаков.

иных предметов, утверждения об этих предметах и т. п.) суть слова в этом алфавите; каждую русскую фразу, например, и даже каждый русский текст можно рассматривать как слово в алфавите, представляющем собой расширение указанного выше 66-буквенного алфавита за счет знаков препинания, знака пробела между словами, знака абзацного отступа (и, быть может, еще некоторых знаков). Предполагая, что выражения языка являются словами в некотором алфавите, мы тем самым налагаем запрет на такое «многоэтажное» выражение, как, например, $\int_a^0 f(x)\,dx$. Этот запрет, однако, не является слишком ограничительным, поскольку все подобные выражения можно при подходящей кодировке «вытянуть в строку». Всякое множество M такое, что $M \subseteq Б^\infty$, называется *словарным в* Б. Просто *словарным* называется множество, словарное в каком-либо алфавите. Сделанное только что предположение может быть теперь сформулировано короче: множество выражений всякого языка словарно.

1.2. Множество истинных утверждений. Предполагается, что в множестве $Б^\infty$, где Б — алфавит рассматриваемого языка, задано подмножество T, называемое множеством «истинных утверждений» (или, короче, просто «истин»). Таким образом, мы опускаем все промежуточные этапы, посредством которых, во-первых, среди слов в алфавите Б выделяются правильно построенные *выражения* языка, получающие определенный смысл при интерпретации (такие, как $2+3$, $x+3$, $x=y$, $x=3$, $2=3$, $2=2$, — в отличие от таких, как $+=x$); во-вторых, среди выражений выделяются так называемые *формулы*, означающие при интерпретации «утверждения, зависящие, быть может, от параметра» (такие, как $x=3$, $x=y$, $2=3$, $2=2$); в-третьих, среди формул выделяются так называемые *замкнутые формулы*, или утверждения, не зависящие от параметра (такие, как $2=3$, $2=2$); и лишь, в-четвертых, среди утверждений выделяются *истинные утверждения* (такие, как $2=2$).

1.3. Для наших целей будет достаточным считать язык полностью заданным, коль скоро задан алфавит Б и подмножество T множества $Б^\infty$. Всякую такую пару $\langle Б, T\rangle$ мы будем называть *фундаментальной парой*.

2. **Недоказуемое.** «Недоказуемое» значит не являющееся доказуемым, а «доказуемое» значит имеющее доказательство.

3. **Доказательство.** Хотя термин «доказательство» является едва ли не самым главным в математике[1]), он не имеет точного определения. Понятие доказательства во всей его полноте принадлежит математике не более чем психологии: ведь доказательство — это просто рассуждение, убеждающее нас настолько, что с его помощью мы готовы убеждать других.

3.1. Будучи записанным, доказательство становится словом в некотором алфавите Д (вспомним, что говорилось выше о русских текстах); все доказательства образуют некую (достаточно, впрочем, расплывчатую) совокупность в $Д^\infty$. Не претендуя на то, чтобы дать точное определение для такого «наивного» или «абсолютного» понятия доказательства (или, что то же самое, для соответствующей совокупности в $Д^\infty$), мы займемся его формальным аналогом, для которого, однако, сохраним тот же термин «доказательство». Этот аналог в двух существенных чертах будет отличаться от интуитивного понятия[2]): во-первых, мы будем допускать существование разных понятий «доказательства» (что приведет к различным подмножествам в множестве $Д^\infty$, да и сам алфавит Д может варьироваться); во-вторых, для каждого из таких понятий мы будем требовать наличия эффективного способа, или алгоритма[3]), проверки, является ли данное слово в алфавите Д доказательством или нет. Далее, будем предполагать наличие алгоритма, который по доказательству определяет, доказательством какого утверждения оно является. (В обычных случаях этим утверждением является последнее утверждение в цепочке, образующей доказательство.)

3.2. Итак, окончательное определение таково:

1° Имеются алфавиты Б (*алфавит языка*) и Д (*алфавит доказательств*).

---

[1]) Н. Бурбаки начинает свои «Начала математики» словами «Со времен греков говорить «математика» — значит говорить «доказательство».

[2]) Впрочем, и интуитивное понятие не вовсе лишено этих черт.

[3]) Этот термин уточняется в следующем параграфе.

2° В множестве $Д^\infty$ выделено подмножество D, элементы которого называются *доказательствами*; предполагается наличие алгоритма, позволяющего по произвольному слову в алфавите Д узнавать, принадлежит оно D или нет.

3° Имеется функция δ (*функция выделения доказанного*), у которой область определения Δ удовлетворяет соотношению $D \subseteq \Delta \subseteq Д^\infty$ и которая принимает свои значения в $Б^\infty$; предполагается наличие алгоритма, вычисляющего[1]) эту функцию; доказательство d из D называется доказательством слова $\delta(d)$.

3.3. Тройку $\langle Д, D, \delta \rangle$, удовлетворяющую условиям 1°—3°, назовем *дедуктикой* над алфавитом Б.

3.4. Для читателей, знакомых с обычными способами задания понятия «доказательство» посредством «аксиом» и «правил вывода», поясним, почему эти способы могут быть рассмотрены как частный случай определения из п. 3.2. В самом деле, доказательством обычно называют цепочку выражений языка, в которой каждый член или является аксиомой, или получается из предыдущих по одному из правил вывода. Добавляя к алфавиту языка новую букву $*$, мы можем записывать доказательства в виде слов в расширенном таким образом алфавите: цепочка $\langle C_1, \ldots, C_n \rangle$ изображается словом $C_1 * C_2 * \ldots * C_n$. Функция выделения доказанного выделяет из каждого слова наибольший не содержащий буквы $*$ конец. Требуемые определением из п. 3.2 алгоритмы могут быть легко построены для любого обычно рассматриваемого уточнения понятий «быть аксиомой» и «получаться по одному из правил вывода».

4. Попытки уточнения первоначальной формулировки.

4.1. П е р в а я п о п ы т к а. При определенных условиях для фундаментальной пары $\langle Б, T \rangle$ и дедуктики $\langle Д, D, \delta \rangle$ над Б существует слово из T, не имеющее доказательства. Такая формулировка еще слишком неопределенна. К тому же ясно, что можно придумать много дедуктик, в каждой из которых будет очень мало доказуемых слов. В пустой дедуктике (где $D = \varnothing$) вообще нет ни одного доказуемого слова.

---

[1]) Что означают слова «алгоритм вычисляет функцию», будет уточнено в следующем параграфе.

4.2. Вторая попытка. Более естественным является другой подход. Задан некоторый язык в том точном смысле, что задана фундаментальная пара $\langle Б, T \rangle$. Мы теперь ищем дедуктики над Б (содержательно — ищем такие способы доказывания), в которых доказывалось бы как можно больше слов из T, в идеале — все слова из T. Нас интересует ситуация, когда такой дедуктики (в которой каждое слово из T имело бы доказательство) не существует. Итак, нас заинтересовала бы следующая формулировка: при определенных условиях, налагаемых на фундаментальную пару $\langle Б, T \rangle$, не существует дедуктики над Б, в которой каждое слово из T имеет доказательство. Однако пары $\langle Б, T \rangle$ с этим свойством просто не может быть. В самом деле, достаточно положить $Д = Б$, $D = Д^{\infty}$, $\delta(d) = d$ для всякого d из $Д^{\infty}$; тогда всякое слово из $Б^{\infty}$ окажется доказуемым (его доказательством будет оно само).

5. **Непротиворечивость.** Естественно потребовать, чтобы доказуемыми были лишь «истинные утверждения», т. е. слова, принадлежащие множеству T. Назовем дедуктику $\langle Д, D, \delta \rangle$ *непротиворечивой относительно* (или *для*) фундаментальной пары $\langle Б, T \rangle$, коль скоро $\delta(D) \subseteq T$. В дальнейшем будем интересоваться лишь непротиворечивыми дедуктиками. Если имеется язык, то представляется весьма заманчивым найти такую непротиворечивую дедуктику, в которой каждое истинное утверждение было бы доказуемым. Теорема Гёделя в интересующем нас варианте именно и утверждает, что при определенных условиях, налагаемых на фундаментальную пару, этого сделать нельзя.

6. **Полнота.** Назовем дедуктику $\langle Д, D, \delta \rangle$ *полной относительно* (или *для*) фундаментальной пары $\langle Б, T \rangle$, коль скоро $\delta(D) \supseteq T$. Занимающая нас формулировка приобретает такой вид:

при определенных условиях, налагаемых на фундаментальную пару $\langle Б, T \rangle$, *не существует дедуктики над* Б, *полной и непротиворечивой относительно* $\langle Б, T \rangle$.

На этой формулировке мы и остановимся и в следующих параграфах найдем те условия, о которых в ней идет речь.

§ 2. НАЧАЛЬНЫЕ ПОНЯТИЯ ТЕОРИИ АЛГОРИТМОВ И ИХ ПРИМЕНЕНИЯ

Условия, при которых не существует полной непротиворечивой дедуктики, легко формулируются в терминах теории алгоритмов.

Нам достаточно на первых порах лишь самых общих интуитивных представлений об *алгоритме* как о предписании, позволяющем по каждому *исходному данному*, или *аргументу*, из некоторой совокупности *возможных* (для данного алгоритма) *исходных данных* (аргументов) получить *результат* в случае, если таковой существует, или не получить ничего в случае, если для рассматриваемого исходного данного не существует результата[1]). Если для выбранного исходного данного результат существует, говорят, что алгоритм *применим* к этому исходному данному и *перерабатывает* его в этот результат.

Для наших целей будет достаточным — и это позволит избежать лишних обсуждений — считать, что исходные данные и результаты любого алгоритма суть слова. Более точно: для каждого алгоритма можно указать некоторый *алфавит исходных данных*, так что все возможные исходные данные являются словами в этом алфавите, и некоторый *алфавит результатов*, так что все результаты являются словами в этом алфавите. Поэтому, чтобы иметь дело с алгоритмами, применяемыми, скажем, к парам слов или к цепочкам слов, мы должны предварительно записать эти образования в виде слов в каком-нибудь алфавите. Для определенности условимся соотносить с каждым алфавитом Б некоторую не входящую в него букву и обозначать эту букву звездочкой (подчеркнем, что, таким образом, эта звездочка в различных ситуациях обозначает различные буквы). Первоначальный алфавит Б, пополненный этой новой буквой, будем обозначать $Б_*$. В п. 3.4 предыдущего параграфа мы уже договорились записывать цепочку $\langle C_1, \ldots, C_n \rangle$ слов в алфавите Б посредством слова $C_1 * \ldots * C_n$ в алфавите $Б_*$; в частности, в том же $Б_*$ запишется в виде слова $C_1 * C_2$ и пара $\langle C_1, C_2 \rangle$. Пусть, далее, при фиксирован-

[1]) Подчеркнем, что возможные исходные данные — это не те данные, в применении к которым алгоритм дает результат, а те, к которым можно его применять (возможно, безрезультатно).

ном n $Б_1$, $Б_2$, ..., $Б_n$ суть произвольные алфавиты; обозначая по-прежнему через $*$ дополнительную букву, соотнесенную с алфавитом $(Б_1 \cup \ldots \cup Б_n)$ и тем самым заведомо не входящую ни в один из $Б_i$, мы будем отождествлять цепочку $\langle C_1, \ldots, C_n \rangle$, где каждое C_i является словом в $Б_i$, со словом $C_1 * \ldots * C_n$ в алфавите $(Б_1 \cup \ldots \cup Б_n)_*$; совокупность всех таких цепочек (и отождествленных с ними слов) будем обозначать через $Б_1^\infty \times \ldots \times Б_n^\infty$.

Совокупность всех исходных данных, к которым алгоритм применим, называется *областью применимости* алгоритма; каждый алгоритм задает функцию, относящую каждому элементу области применимости соответствующий результат; область определения этой функции совпадает, таким образом, с областью применимости алгоритма; говорят, что рассматриваемый алгоритм *вычисляет* функцию, задаваемую указанным способом. Условимся обозначать через $\boldsymbol{A}(x)$ результат применения алгоритма $\boldsymbol{A}$ к объекту x (при этом $\boldsymbol{A}(\langle x_1, x_2, \ldots, x_n \rangle)$ для краткости будем записывать просто как $\boldsymbol{A}(x_1, \ldots, x_n)$). Тогда определение термина «вычисляет» можно переформулировать следующим образом: алгоритм $\boldsymbol{A}$ вычисляет функцию f, коль скоро $\boldsymbol{A}(x) \simeq f(x)$ для всех x. (Знак $\simeq$ есть знак «условного равенства»; утверждение $A \simeq B$ считается истинным в двух случаях: либо когда выражения A и B оба не определены, либо когда A и B оба определены и обозначают одно и то же.)

Функция, которая вычисляется некоторым алгоритмом, называется *вычислимой*. В части 3° определения понятия доказательства (п. 3.2 предыдущего параграфа) говорится, следовательно, о том, что функция выделения доказанного должна быть вычислимой функцией.

В силу сделанных предположений относительно понятия алгоритма для каждой вычислимой функции можно указать такие два алфавита, что все ее аргументы суть слова в первом из этих алфавитов, а все ее значения — слова во втором из этих алфавитов.

Особый интерес представляют функции, аргументы и значения которых суть натуральные числа [1]). Такие функции условимся называть *числовыми*. Чтобы иметь

---

[1]) Число 0 мы также считаем натуральным.

право говорить о вычислимых числовых функциях, мы должны ввести в рассмотрение алгоритмы, имеющие дело с числами, а для этого прежде всего необходимо представить числа в виде слов в каком-либо алфавите, называемом в этом случае *цифровым*. Возможны различные способы такого представления, например: 1) двоичная запись чисел в алфавите $\{0, 1\}$; 2) десятичная запись чисел в алфавите $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$; 3) запись чисел в однобуквенном алфавите $\{|\}$, причем число n записывается словом $\underbrace{||\ldots|}_{n \text{ раз}}$; 4) запись чисел в трехбуквенном алфавите $\{|, (,)\}$, причем число n записывается словом $(\underbrace{||\ldots|}_{n \text{ раз}})$, и т. д. Для тех или иных целей выбираются наиболее удобные способы записи. Каждая запись числа (в какой-либо фиксированной системе) называется *цифрой*. Допуская вольность речи, говорят об алгоритмах и вычислимых функциях, оперирующих с числами, имея в виду алгоритмы и вычислимые функции, оперирующие с изображающими эти числа цифрами (в какой-либо выбранной системе записи).

Понятие вычислимой числовой функции, таким образом, выглядит зависящим от принятого способа записи чисел. Однако легко обнаружить, что всякая числовая функция, вычислимая при одной системе записи. будет вычислима и при другой, по крайней мере для широкого класса таких систем. Назовем две системы эквивалентными, если существует алгоритм, дающий по записи произвольного числа в первой системе запись этого же числа во второй системе, а также алгоритм, дающий по записи произвольного числа во второй системе запись этого же числа в первой системе. Приведенные выше примеры систем записи очевидным образом эквивалентны. Покажем, что числовая функция f, вычислимая при одной из двух эквивалентных систем записи, вычислима и при другой системе. Пусть $\boldsymbol{C}$ и $\boldsymbol{D}$ — алгоритмы перехода от первой системы ко второй и обратно, и пусть алгоритм $\boldsymbol{A}$ вычисляет функцию f при первой системе записи (т. е. $\boldsymbol{A}$ вычисляет функцию на цифрах первой системы, индуцированную функцией f). Тогда следующий алгоритм $\boldsymbol{B}$ будет вычислять f при второй системе записи (т. е. вычислять

индуцированную функцию на цифрах второй системы):

$$B(x) \simeq CAD(x).$$

Предписание, задающее алгоритм B, может быть словесно выражено следующим образом: «переведи x в первую систему счисления, затем примени алгоритм A, полученный результат (если таковой получится) переведи обратно во вторую систему счисления». Аналогичным образом вводимое ниже понятие перечислимого числового множества не зависит от выбора системы записи чисел.

Ввиду сказанного мы позволим себе, коль скоро фиксирована какая-либо система записи чисел, не слишком педантично различать числа и цифры; множество и тех и других будем называть натуральным рядом и обозначать буквой $\mathbb{N}$.

Множество называется *перечислимым*, если оно либо пусто, либо является множеством элементов какой-нибудь вычислимой последовательности (т. е. множеством значений какой-нибудь вычислимой функции, определенной на натуральном ряду); о такой функции (последовательности) говорят, что она *перечисляет* рассматриваемое множество. Очевидно, каждое перечислимое множество словарно.

Пример 1. Множество $\mathbb{N}^2$ всевозможных пар натуральных чисел перечислимо: одна из перечисляющих функций — функция

$$\varphi(n) = \langle a, b \rangle, \quad \text{где} \quad n = 2^a(2b+1) - 1.$$

Пример 2. Множество $Ж^\infty$ всех слов в произвольном алфавите Ж перечислимо. Один из возможных способов построения перечисляющей последовательности таков: упорядочиваем произвольным образом элементы Ж; затем слова в Ж упорядочиваем следующим образом: из слов разной длины предшествующим считается то, которое короче, а на словах одинаковой длины вводим словарный порядок (сравнивая два слова, находим первые слева различающиеся буквы и смотрим, какая из них идет раньше в упорядочении алфавита Ж). Выписывая слова в порядке следования друг за другом, получаем требуемую перечисляющую последовательность. (Может возникнуть вопрос, почему она вычислима, т. е. почему существует алгоритм, дающий по k член a_k этой

последовательности с номером k; искомый алгоритм, например, таков: выписывай члены последовательности, пока их не станет $k+1$; последний из выписанных членов и будет a_k[1]).)

Пример 3. Вычислимая функция f, перечисляющая $Ж^\infty$ и построенная в примере 2, осуществляет взаимно однозначное отображение $\mathbb{N}$ на $Ж^\infty$; поэтому можно говорить об обратной функции f^{-1}, осуществляющей взаимно однозначное отображение $Ж^\infty$ на $\mathbb{N}$. Эта f^{-1} тоже вычислима, поскольку вычисляется следующим алгоритмом: чтобы вычислить $f^{-1}(a)$, вычисляй последовательно $f(0), f(1), f(2), \ldots$ и т. д., пока для некоторого n не получишь $f(n)=a$; это n и есть $f^{-1}(a)$.

Пример 4. Для любых алфавитов $Ж_1$ и $Ж_2$ композиция вычислимых функций, взаимно однозначно отображающих $\mathbb{N}$ на $Ж_2^\infty$ (пример 2) и $Ж_1^\infty$ на $\mathbb{N}$ (пример 3), дает вычислимую же функцию, взаимно однозначно отображающую $Ж_1^\infty$ на $Ж_2^\infty$.

Подмножество S множества A называется *разрешимым* относительно A, коль скоро существует такой алгоритм (*разрешающий* S относительно A), который распознает принадлежность элементов A к S, т. е. такой алгоритм, который все элементы из S перерабатывает в некоторое одно и то же слово x (например, в слово «да»), а все элементы из $A \setminus S$ в некоторое одно и то же, но отличное от x слово y (например, в слово «нет»; разумеется, выбор слов x и y совершенно несуществен). Очевидно, разрешимость множества S относительно A равносильна разрешимости множества $A \setminus S$ относительно того же A. В части 2° определения понятия доказательства требовалось, чтобы множество всех доказательств было разрешимо относительно множества всех слов в алфавите доказательств.

Из определения разрешимости вытекает, что область применимости алгоритма, разрешающего S относительно A, объемлет A. При этом безразлично, что получается в результате применения алгоритма к словам, не лежащим в A. Например, если мы хотим построить алгоритм, отличающий стихи Пушкина от

[1]) Напомним, что последовательность начинается с a_0.

стихов Лермонтова, и тем самым доказать разрешимость множества стихов Пушкина относительно множества стихов Пушкина и Лермонтова, то нам неважно, что получится (и получится ли что-нибудь вообще) в результате применения этого алгоритма к стихотворению Маяковского или к Уставу гарнизонной и караульной служб. Возникает естественный вопрос: что произойдет, если предложить другое, более узкое определение разрешимости, потребовав, чтобы разрешающий алгоритм был применим *только* к элементам множества A? При таком определении разрешимость S относительно A равносильна, очевидно, вычислимости характеристической функции множества S относительно A (т. е. определенной на A функции, равной 1 на S и 0 на $A \setminus S$). Как будет показано в § 5 (следствие 1 аксиомы протокола), область применимости любого алгоритма всегда есть перечислимое множество, и потому лишь перечислимые множества могут обладать разрешимыми — в смысле нового, узкого определения — подмножествами. Если же множество A перечислимо, то для него оба определения разрешимого подмножества приводят к одинаковым результатам. В самом деле, пусть вычислимая функция f перечисляет A, а алгоритм $\boldsymbol{B}$ разрешает S относительно A в прежнем, широком смысле. Тогда следующий алгоритм будет также разрешать S относительно A и притом иметь A своею областью применимости: бери произвольное a и вычисляй последовательно $f(0)$, $f(1)$, $f(2)$, ... ; как только получишь $f(n) = a$, применяй к a алгоритм $\boldsymbol{B}$.

Замечание 1. Поскольку каждая вычислимая функция, каждое перечислимое множество и каждое разрешимое подмножество задаются некоторым алгоритмом, существование функций, множеств и подмножеств, не являющихся соответственно вычислимыми, перечислимыми или разрешимыми[1]), усматриваются из количественных соображений. Действительно, каждый алгоритм может быть записан в конечном счете на русском языке (с добавлением, если надо, необходимых математических символов), т. е., согласно

[1]) Имеются в виду, конечно, утверждения о существовании неперечислимых словарных множеств, невычислимых функций со словарными областями определения и значений и т. п.

п. 1.1 предыдущего параграфа, в виде слова в некотором достаточно обширном алфавите, а всех слов в произвольном алфавите — счетное множество. Конечно, от такого рассуждения еще далеко до построения индивидуальных примеров неалгоритмических объектов.

Приложим теперь описанные только что понятия теории алгоритмов к исследованию возможности существования полной непротиворечивой дедуктики.

Лемма 1. *Каково бы ни было словарное множество X, множества $\varnothing$ и X разрешимы относительно X.*

Доказательство. Пусть X словарно в Ж. Достаточно взять алгоритм, который каждому слову из Ж$^\infty$ ставит в соответствие некоторое одно и то же слово x. Этот алгоритм будет разрешать каждое из множеств $\varnothing$ и X относительно X.

Теорема 1. *Если T — перечислимое множество, то для фундаментальной пары $\langle$Б, $T\rangle$ можно ввести полную непротиворечивую дедуктику.*

Доказательство. Требуется задать тройку $\langle$Д, $D, \delta\rangle$. Замечаем, что $\varnothing$ и Д$^\infty$ разрешимы (относительно Д$^\infty$) по лемме 1. Если $T = \varnothing$, то берем $\langle$Д, $\varnothing, \delta\rangle$, где Д и δ — любые. Если $T \neq \varnothing$, то $T = \{\tau(0), \tau(1), \tau(2), \ldots\}$, где τ — вычислимая функция; отождествим число n со словом $\|\ldots|$ длины n и положим Д $= \{\ |\ \}$, $D =$ Д$^\infty$, $\delta = \tau$.

Замечание 2. Это доказательство не такое искусственное, как может показаться на первый взгляд. В самом деле, если множество истин некоторого языка перечислимо, т. е. может быть расположено в вычислимую последовательность, то для того, чтобы убедиться в принадлежности какого-либо выражения к этому множеству (т. е. доказать истинность рассматриваемого выражения), достаточно указать номер этого выражения в этой последовательности (каковой номер поэтому и можно считать доказательством). Обратное к теореме 1 утверждение будет доказано дальше (теорема 3); предварительно нам придется доказать некоторые вспомогательные утверждения.

Лемма 2 (о перечислимости разрешимого подмножества). *Разрешимое подмножество перечислимого множества перечислимо.*

Доказательство. Пусть $S \subseteq A$, причем A перечисляется вычислимой функцией f. Если S пусто, то S

перечислимо по определению. Если S непусто, то существует такое s, что $s \in S$. Положим

$$g(n) = \begin{cases} f(n), & \text{если } f(n) \in S, \\ s, & \text{если } f(n) \in A \setminus S. \end{cases}$$

Очевидно, g есть вычислимая функция, перечисляющая множество S.

Из леммы 2 вытекает, что всякое разрешимое подмножество натурального ряда перечислимо. Однако обратное утверждение неверно: в § 5 будет построен пример перечислимого неразрешимого подмножества натурального ряда. Следующая лемма указывает условия разрешимости перечислимого множества.

Лемма 3. *Подмножество S перечислимого множества X тогда и только тогда разрешимо относительно X, когда перечислимо как S, так и его дополнение $X \setminus S$.*

Доказательство. Если S разрешимо, то разрешимо и $X \setminus S$, и остается применить лемму 2 о перечислимости разрешимого множества. Пусть теперь S и $X \setminus S$ оба перечислимы. Если хотя бы одно из них пусто, то по лемме 1 множество S разрешимо. Если оба они непусты, то, стало быть, перечисляются некоторыми вычислимыми функциями f и g. Тогда, чтобы ответить на вопрос «$x \in S$?», поставленный для произвольного x из X, достаточно вычислять последовательно

$$f(0), \quad g(0), \quad f(1), \quad g(1), \quad \ldots$$

до тех пор, пока не встретится x (что произойдет непременно, так как образующаяся последовательность исчерпывает все X). Если при этом окажется, что x встретилось среди значений f, то x принадлежит S; если же x встретилось среди значений g, то x не принадлежит S.

Теорема 2. *Множество всех доказательств (для данной дедуктики) перечислимо.*

Доказательство. Множество всех слов в алфавите доказательств перечислимо (см. пример 2). Поэтому достаточно применить лемму 2.

Лемма 4 (об образе перечислимого множества). *Пусть R перечислимо и f — вычислимая функция, определенная на всех элементах множества R. Тогда $f(R)$ перечислимо.*

Доказательство. Если R пусто, то и $f(R)$ пусто. Если R перечисляется вычислимой функцией ρ, то $f(R)$ перечисляется вычислимой функцией $y = f(\rho(x))$.

Пример 5. Пусть $\neg$ — символ алфавита Л, $A \subseteq Л^\infty$. Обозначим через $\neg A$ множество всех слов вида $\neg a$, где $a \in A$. Полагая в лемме 4 $R = A$, $f(a) = \neg a$, получаем, что из перечислимости A вытекает перечислимость $\neg A$; полагая $R = \neg A$, $f(\neg a) = a$, получаем, что из перечислимости $\neg A$ вытекает перечислимость A.

Пример 6. Для любого алфавита И множество $И^\infty \times И^\infty$ перечислимо. В самом деле, множества $\mathbb{N}^2$ и $И^\infty$ перечислимы (примеры 1 и 2). Пусть $И^\infty$ перечисляется вычислимой последовательностью g. Определим на $\mathbb{N}^2$ вычислимую функцию f, полагая $f(a, b) = \langle g(a), g(b) \rangle$. Очевидно, $f(\mathbb{N}^2) = И^\infty \times И^\infty$ и остается применить лемму 4.

Как обычно, через $K_1 \times K_2 \times \ldots \times K_n$ обозначается прямое произведение множеств $K_1, \ldots, K_n$, т. е. множество всех таких цепочек $\langle k_1, \ldots, k_n \rangle$, что $k_1 \in K_1, \ldots, k_n \in K_n$. В силу соглашений, сделанных в начале параграфа, в случае, если $K_1 \subseteq Б_1^\infty, \ldots, K_n \subseteq Б_n^\infty$, где $Б_1, \ldots, Б_n$ — алфавиты, прямое произведение $K_1 \times \ldots \times K_n$ отождествляется с некоторым множеством слов из $Б_1^\infty \times \ldots \times Б_n^\infty$.

Следствие 1 леммы 4. *Если $K_1, \ldots, K_n$ суть перечислимые множества, то их прямое произведение $K_1 \times \ldots \times K_n$ также перечислимо.*

Доказательство. Для $n = 2$ — как в примере 6. Далее — по индукции, применяя лемму 4 к «естественному» вычислимому отображению множества $(K_1 \times \ldots \times K_s) \times K_{s+1}$ на множество $K_1 \times \ldots \times K_s \times K_{s+1}$.

Цепочка $\langle C_{i_1}, \ldots, C_{i_r} \rangle$, где $i_1 \leqslant n, \ldots, i_r \leqslant n$, называется *проекцией* цепочки $\langle C_1, \ldots, C_n \rangle$ на оси $i_1, \ldots, i_r$ и обозначается $пр_{i_1, \ldots, i_r} \langle C_1, \ldots, C_n \rangle$. В частности, $пр_1 \langle C_1, \ldots, C_n \rangle = C_1$, $пр_2 \langle C_1, \ldots, C_n \rangle = C_2$. Если $M \subseteq K_1 \times \ldots \times K_n$, то через $пр_{i_1, \ldots, i_r} M$ обозначается множество всевозможных проекций $пр_{i_1, \ldots, i_r} m$, где $m \in M$.

Следствие 2 леммы 4. *Если M — перечислимое подмножество множества* $Б_1^\infty \times \ldots \times Б_n^\infty$, *где*

$Б_1, \ldots, Б_n$ — *некоторые алфавиты, а* $i_1, \ldots, i_r$ — *числа, не превосходящие* n, *то* $\text{пр}_{i_1,\ldots,i_r}M$ *перечислимо.*

Доказательство. Достаточно рассмотреть вычислимую функцию $x \mapsto \text{пр}_{i_1,\ldots,i_r}x$.

Теорема 3. *Множество всех доказуемых слов (для данной дедуктики) перечислимо.*

Доказательство. Пусть P — множество всех доказуемых слов для дедуктики $\langle Д, D, \delta\rangle$. Очевидно, что $P = \delta(D)$. По теореме 2 множество D перечислимо. Остается применить лемму 4.

Таким образом, если T неперечислимо, то для пары $\langle Б, T\rangle$ невозможно ввести полную непротиворечивую дедуктику; для всякой непротиворечивой дедуктики множество доказуемых слов P будет собственным подмножеством множества T и в разности $T \setminus P$ всегда найдется элемент; этот элемент будет истинным, но не доказуемым утверждением!

Теоремы 1 и 3 в совокупности дают условия, налагаемые на фундаментальную пару и необходимые и достаточные для того, чтобы для этой пары можно было ввести полную непротиворечивую дедуктику. Это условие — перечислимость множества всех истин. Можно ожидать (и так и оказывается на самом деле), что в «богатых», «выразительных» языках множества всех истин настолько сложны, что неперечислимы, и потому для этих языков невозможны полные непротиворечивые дедуктики. Найденный критерий, однако, не слишком удобен, поскольку рассмотрение множества T всех истин может оказаться затруднительным. Поэтому мы в следующем параграфе переформулируем этот критерий, сделав его более «применимым».

§ 3. ПРОСТЕЙШИЕ КРИТЕРИИ НЕПОЛНОТЫ

Мы знаем теперь, что неперечислимость множества T необходима и достаточна для того, чтобы для $\langle Б, T\rangle$ не существовало полной и непротиворечивой дедуктики.

Однако нас могут интересовать не все истины языка, а только истины некоторого вида или из некоторого класса, подобно тому как сдающего экзамен по математике интересует истинность не всех математических утверждений, а лишь тех, которые могут встре-

титься на экзамене. Например, может представлять интерес построение дедуктики, в которой выводятся все истинные утверждения длиной не больше 1000 и не выводится ни одного ложного утверждения такой длины. При этом выводимость утверждений большей длины в этой дедуктике может быть никак не связанной с их истинностью. Кроме того, в некоторых случаях (язык теории множеств) множество истин в полном объеме совершенно неопределенно. Сказанное оправдывает рассмотрение понятий непротиворечивости и полноты в применении к произвольному подмножеству множества Б$^\infty$. Перейдем к формальным определениям.

Пусть $\langle$Б, $T\rangle$ — фундаментальная пара, $\langle$Д, D, $\delta\rangle$ — дедуктика над Б и P — множество всех доказуемых слов. Пусть $V \subseteq$ Б$^\infty$. Скажем, что дедуктика $\langle$Д, D, $\delta\rangle$

а) *непротиворечива применительно к* V, если $V \cap P \subseteq V \cap T$;

б) *полна применительно к* V, если $V \cap T \subseteq V \cap P$.

Теорема 4. *Если V — перечислимое подмножество множества Б$^\infty$, а множество истинных утверждений, принадлежащих к V, неперечислимо, то никакая дедуктика не является одновременно непротиворечивой и полной применительно к V.*

Доказательство. По условию $V \cap T$ неперечислимо. Для непротиворечивой и полной применительно к V дедуктики $V \cap T = V \cap P$. Но $V \cap P$ обязано быть перечислимым, как это вытекает из теоремы 3 и следующей леммы.

Лемма 5. *Теоретико-множественные объединение и пересечение перечислимых множеств перечислимы.*

Доказательство. Пусть R и S — перечислимые множества. Сначала докажем перечислимость $R \cup S$. Если одно из множеств пусто, то это тривиально. Если оба множества непусты, то $R = \{\rho(0), \rho(1), \ldots\}$, $S = \{\sigma(0), \sigma(1), \ldots\}$, где ρ и σ — вычислимые последовательности. Тогда вычислимая последовательность f, заданная соотношениями $f(2n) = \rho(n)$, $f(2n+1) = \sigma(n)$, будет перечислять $R \cup S$. Докажем теперь перечислимость $R \cap S$. Если $R \cap S$ пусто, то оно перечислимо по определению. В противном случае существует некоторое a такое, что $a \in R \cap S$, а R и S перечисляются вычислимыми функциями ρ и σ. Поскольку $\mathbb{N}^2$ перечислимо (пример 1 из § 2), оно перечисляется

некоторой вычислимой функцией g. Каждое значение $g(n)$ есть некоторая пара натуральных чисел; обозначим через $\xi(n)$ и $\eta(n)$ первый и второй члены этой пары. Функции ξ и η, очевидно, вычислимы. Введем функцию h:

$$h(n) = \begin{cases} \rho(\xi(n)), & \text{если} \quad \rho(\xi(n)) = \sigma(\eta(n)), \\ a & \text{в противном случае.} \end{cases}$$

Функция h вычислима и перечисляет множество $R \cap S$.

Замечание 1. Условие несуществования дедуктики с определенными свойствами, сформулированное в теореме, является не только достаточным, но и необходимым (причем даже без предположения о перечислимости V). В самом деле, если $V \cap T$ перечислимо, то полная непротиворечивая дедуктика для $\langle$Б, $V \cap T\rangle$, существующая в силу теоремы 1, будет в то же время полной и непротиворечивой для $\langle$Б, $T\rangle$ применительно к V.

Очевидно, что дедуктика непротиворечива (полна) относительно $\langle$Б, $T\rangle$ тогда и только тогда, когда она непротиворечива (полна) применительно к любому подмножеству множества Б^∞. Поэтому для обнаружения неполноты относительно $\langle$Б, $T\rangle$ непротиворечивой (относительно той же $\langle$Б, $T\rangle$) дедуктики достаточно (и необходимо) указать такое подмножество V множества Б^∞, применительно к которому эта дедуктика неполна. Следующее построение помогает найти в ряде важных случаев такое подмножество.

Условимся говорить, что посредством фундаментальной пары $\langle$Б, $T\rangle$ *выразима принадлежность* к множеству Q натуральных чисел, если существует такая определенная на натуральном ряду и принимающая значения в Б^∞ вычислимая функция f (*выражающая* эту принадлежность), что:

1) если $n \in Q$, то $f(n) \in T$,

2) если $n \in \mathbb{N} \setminus Q$, то $f(n) \in \text{Б}^\infty \setminus T$.

Для такой функции f множество V всех ее значений перечислимо. Поэтому (в силу теоремы 4) не будет существовать полной и непротиворечивой применительно к V дедуктики, коль скоро множество $V \cap T$ принадлежащих к V истинных утверждений неперечислимо. Неперечислимость же множества $V \cap T$, как мы сейчас увидим, будет иметь место, если неперечислимо множество Q.

Лемма 6 (о полном прообразе). *Пусть f — вычислимая функция, область определения которой есть перечислимое множество*[1]), *и B — произвольное перечислимое множество. Тогда множество $f^{-1}(B)$ перечислимо.*

Доказательство. Если $f^{-1}(B)$ пусто, оно перечислимо по определению. Пусть теперь $c \in f^{-1}(B)$, множество B перечисляется вычислимой функцией h, а область определения функции f — вычислимой функцией g. Для построения перечисления $f^{-1}(B)$ мы поступаем так.

Перебирая $\mathbb{N} \times \mathbb{N}$, для каждой пары $\langle k, l \rangle$ проверяем, переводит ли функция f элемент $g(k)$ («k-й элемент в перечислении области определения f») в $h(l)$ («l-й элемент в перечислении B»); если да, то включаем $g(k)$ в строимое нами перечисление множества $f^{-1}(B)$, если нет, то включаем в него элемент c.

Более формально, пусть ξ и η определены, как в доказательстве леммы 5. Положим

$$\varphi(n) = \begin{cases} g(\xi(n)), & \text{если} \quad f(g(\xi(n))) = h(\eta(n)), \\ c & \text{в противном случае.} \end{cases}$$

Легко видеть, что φ — вычислимая функция, перечисляющая множество $f^{-1}(B)$.

Вернемся теперь к рассмотрениям, предшествующим формулировке леммы 6. Заметим, что $Q = f^{-1}(V \cap T)$. Поэтому если Q неперечислимо, то неперечислимо и $V \cap T$ (в противном случае в силу леммы 6 было бы перечислимо и Q). Таким образом (принимая во внимание теорему 4) нами доказана следующая

Теорема 5. *Если посредством фундаментальной пары $\langle$Б, $T\rangle$ выразима принадлежность хотя бы к одному неперечислимому множеству натуральных чисел, для $\langle$Б, $T\rangle$ не может существовать непротиворечивой и полной дедуктики; более того, не существует дедуктики, являющейся одновременно непротиворечивой и*

---

[1]) На самом деле область определения всякой вычислимой функции является перечислимым множеством; однако установление этого факта требует дополнительных уточнений наших представлений об алгоритмах, которые будут произведены лишь в § 5.

полной применительно к множеству значений функции, выражающей указанную принадлежность.

Замечание 2. Достаточное условие несуществования, сформулированное в теореме 5, является и необходимым. В самом деле, если для $\langle Б, T \rangle$ нельзя ввести полную непротиворечивую дедуктику, то T неперечислимо (теорема 1); $Б^\infty$ перечислимо (пример 2 из § 2) и перечисляется некоторой вычислимой функцией f. Поскольку $T = f(f^{-1}(T))$, то множество $f^{-1}(T)$ неперечислимо (в силу теоремы 3 об образе перечислимого множества). В то же время функция f выражает принадлежность к $f^{-1}(T)$ посредством пары $\langle Б, T \rangle$.

§ 4. ЯЗЫК АРИФМЕТИКИ

В этом параграфе мы приложим построения предыдущих параграфов к языку арифметики. Содержательно, под языком арифметики понимается язык, утверждения которого формулируются (с помощью логических операций и отношения равенства) в терминах натуральных чисел и операций сложения и умножения. На формальном уровне нам надлежит предъявить соответствующую фундаментальную пару. Разумеется, задача построения такой пары не может иметь однозначного решения: ясно, что возможны различные алфавиты для записи одной и той же сути. Здесь будет избран 14-буквенный алфавит А (арифметический алфавит), буквами которого служат следующие знаки:

1°—2° скобки (и);

3° знак для образования цифр |;

4° знак для образования переменных x;

5°—6° знаки сложения $+$ и умножения $\cdot$;

7° знак равенства $=$;

8°—14° логические знаки $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\exists$, $\forall$ (при содержательной интерпретации эти знаки будут иметь следующий смысл: «неверно, что», «и», «или», «если..., то», «эквивалентно», «существует такой.., что», «для всех»).

Чтобы выделить надлежащее множество истинных утверждений, нам придется предпринять вначале некоторые рассмотрения синтаксического характера: мы должны будем выделить определенные классы слов в $А^\infty$ и заняться их строением.

Слово вида $\underbrace{\alpha \ldots \alpha}_{n \text{ раз}}$, где α — какая-то буква, будем обозначать через α^n. При $n = 0$ слово α^n пусто — не содержит ни одной буквы. *Цифрами* будем называть слова вида $(|^n)$, где $n \geqslant 0$, а *переменными* — слова вида (x^n), где $n > 0$. При интерпретации языка слово $(|^n)$ будет служить записью числа n, а слово (x^n) будет одной из переменных, пробегающих натуральный ряд (для записи утверждений арифметики может потребоваться сколь угодно много таких переменных). Введем теперь следующее индуктивное определение *терма*:

1° все цифры и все переменные суть термы;

2° если t и u — термы, то $(t + u)$ и $(t \cdot u)$ суть термы.

Параметрами терма будем называть все переменные, входящие в него. Терм, не имеющий параметров, будем называть *постоянным*.

Пример 1. Терм $((\,|||\,) \cdot (\,||\,))$ — постоянный, а термы, $((\quad) \cdot (x))$ и $((\,|||\,) + (xx))$ — не постоянные: параметром первого из них является (x), параметром второго — (xx).

Каждому постоянному терму естественно поставить в соответствие число, его *значение*, по следующим правилам:

1° значением цифры $(|^n)$ является число n;

2° значением постоянного терма $(t + u)$ служит сумма значений постоянных термов t и u, а значением постоянного терма $(t \cdot u)$ служит произведение значений постоянных термов t и u.

Пример 2. Значением постоянного терма $((\,|||\,) + ((\,|\,) \cdot (\,||\,)))$ служит число 5.

Всякое слово вида $(t = u)$, где t и u суть термы, будем называть *элементарной формулой*. Наконец, введем следующее индуктивное определение *формулы*:

1° все элементарные формулы суть формулы;

2° если α есть формула, то $\neg\alpha$ есть формула;

3° если α и β суть формулы, то $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$ и $(\alpha \leftrightarrow \beta)$ суть формулы;

4° если α есть формула, а ξ есть переменная, то $\exists\xi\alpha$ и $\forall\xi\alpha$ суть формулы.

Пример 3. Слово

$$(\exists (x) \forall (xx) \neg ((x) = (xx)) \leftrightarrow \forall (xx) ((x) = (xx)))$$

является формулой.

Для облегчения чтения мы будем в дальнейшем записывать термы и формулы сокращенно, заменяя $(|^n)$ на n, (x^n) на x_n и опуская внешние скобки; например, формула из примера 3 может быть сокращенно записана так:

$$\exists x_1 \forall x_2 \neg (x_1 = x_2) \leftrightarrow \forall x_2 (x_1 = x_2).$$

Среди формул и будут выделяться истинные утверждения. Но сначала нам потребуются сравнительно более технические понятия параметров формулы и подстановки цифры вместо переменной.

Мы сопоставим каждой формуле некоторое конечное множество переменных, элементы которого будут называться *параметрами* формулы. Множества параметров формул определяются индуктивно по следующим правилам:

1° параметрами элементарной формулы $(t = u)$ являются все параметры терма t, а также все параметры терма u;

2° у формулы $\neg\alpha$ те же параметры, что у формулы α;

3° параметрами формул $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$ и $(\alpha \leftrightarrow \beta)$ являются все параметры формулы α, а также все параметры формулы β;

4° параметрами формул $\exists\xi\alpha$ и $\forall\xi\alpha$ являются все параметры формулы α, отличные от ξ.

Пример 4. Единственным параметром формулы из примера 3 является x_1. В самом деле, параметрами формулы $(x_1 = x_2)$ являются x_1 и x_2, те же параметры у формулы $\neg(x_1 = x_2)$; параметром формулы $\forall x_2 \neg(x_1 = x_2)$ является x_1, формула $\exists x_1 \forall x_2 \neg(x_1 = x_2)$ не имеет параметров; с другой стороны, единственным параметром формулы $\forall x_2 (x_1 = x_2)$ является x_1.

Менее формально параметры можно описать как переменные, входящие в формулу свободно, т. е. не попадающие в область действия одноименных кванторов.

Формулы, не имеющие параметров, называются *замкнутыми формулами* или *суждениями*[1]). Формула из примера 3 не является суждением. Суждения интерпретируются как высказывания о свойствах натурального ряда; каждому из них приписывается значение «истина» или «ложь» согласно описанному ниже способу (согласующемуся с подразумеваемым смыслом символов, входящих в формулы). Те суждения, которым окажется приписанным значение «истина», и будут служить «истинными утверждениями арифметики».

Пример 5. Предложение «для всякого натурального числа, кроме нуля, найдется меньшее натуральное число» может быть переведено следующей формулой арифметики:

$$\forall x_1(\neg(x_1 = 0) \to \exists x_2 \exists x_3 (\neg(x_3 = 0) \wedge ((x_2 + x_3) = x_1))).$$

Свойство «x_2 меньше x_1» приходится (из-за отсутствия в языке символа $<$) записывать косвенно:

$$\exists x_3 (\neg(x_3 = 0) \wedge ((x_2 + x_3) = x_1)).$$

Прежде чем мы перейдем к установлению значений замкнутых формул, нам понадобится еще одно, на этот раз последнее, техническое понятие — понятие *результата подстановки цифры n вместо переменной w в формулу α*. Этот результат является формулой, обозначается $S_n^w \alpha$ и определяется индуктивно по следующим правилам:

1° результатом подстановки n вместо w в элементарную формулу $(t = u)$ является результат замены всех вхождений переменной w на цифру n;

2° $S_n^w \neg \alpha = \neg S_n^w \alpha$;

3° если λ — любой из символов $\wedge$, $\vee$, $\to$, $\leftrightarrow$, то

$$S_n^w (\alpha \lambda \beta) = (S_n^w \alpha \lambda S_n^w \beta);$$

4° результатом подстановки n вместо w в формулу $Q\xi\alpha$, где Q — один из знаков $\forall$, $\exists$, а ξ — переменная, является формула $Q\xi S_n^w \alpha$, если переменная w отлична от переменной ξ; в противном случае (если w и ξ —

---

[1]) В более продвинутых исследованиях различают суждения и выражающие их замкнутые формулы, но мы оставляем в стороне это различие.

одна и та же переменная) результат будет совпадать с исходной формулой $\mathrm{Q}\xi\alpha$.

Пример 6. Если α — формула из примера 3, то $S^{x_1}_5\alpha$ есть $\exists x_1 \forall x_2 \neg (x_1 = x_2) \leftrightarrow \forall x_2 (5 = x_2)$, а $S^{x_2}_1\alpha$ есть α. Заметим, что если бы мы вместо всех вхождений x_1 в формулу α подставили 5, то получили бы слово $\exists 5 \forall x_2 \neg (5 = x_2) \longrightarrow \forall x_2 (5 = x_2)$, не являющееся формулой. (Согласно нашему определению, при подстановке вместо w следует оставлять без изменений те вхождения, которые попадают под действие кванторов $\exists w$ и $\forall w$.)

Лемма 7. *Параметрами формулы $S^w_n\alpha$ являются параметры формулы α, отличные от w.*

Это очевидное утверждение может быть формально доказано индукцией по построению (или по длине) формулы α.

Теперь мы уже в состоянии перейти к снабжению суждений *значениями*. Как уже говорилось, таких значений будет два — «истина» (*И*) и «ложь» (*Л*). Суждения, имеющие значение *И*, будем называть истинными, имеющие значение *Л* — ложными. Значения формул определяются индукцией по построению формул следующим образом:

1° суждение $(t = u)$ истинно, если значения постоянных термов t и u равны; в противном случае оно ложно;

2° суждение $\neg\alpha$ истинно, если суждение α ложно; в противном случае оно ложно;

3° суждение $(\alpha \wedge \beta)$ истинно, если оба суждения α и β истинны; в противном случае оно ложно;

4° суждение $(\alpha \vee \beta)$ истинно, если хотя бы одно из суждений α и β истинно; в противном случае суждение $(\alpha \vee \beta)$ ложно;

5° суждение $(\alpha \rightarrow \beta)$ ложно, если суждение α истинно, а суждение β ложно; в противном случае суждение $(\alpha \rightarrow \beta)$ истинно;

6° суждение $(\alpha \leftrightarrow \beta)$ истинно, если значения суждений α и β одинаковы; в противном случае суждение $(\alpha \leftrightarrow \beta)$ ложно;

7° суждение $\exists\xi\alpha$ истинно, если существует такая цифра n, что суждение $S^{\xi}_n\alpha$ истинно; если такой цифры нет, то суждение $\exists\xi\alpha$ ложно;

8° суждение $\forall\xi\alpha$ истинно, если для любой цифры n суждение $S_n^\xi\alpha$ истинно; в противном случае суждение $\forall\xi\alpha$ ложно.

Заметим (это относится к 7° и 8°), что $S_n^\xi\alpha$ является суждением, так как формула α не имеет параметров, отличных от ξ (иначе $\exists\xi\alpha$ и $\forall\xi\alpha$ не были бы суждениями).

Пример 7. Формула из примера 5 истинна. Формула из примера 3 не является ни истинной, ни ложной, поскольку не является суждением; однако результат подстановки в нее вместо переменной x_1 любой цифры является истинным суждением.

Истинные суждения мы и объявим истинными утверждениями арифметики. Обозначая их множество буквой T, мы приходим к фундаментальной паре $\langle A, T\rangle$ языка арифметики. Нас будет интересовать возможность ввести для этой пары полную непротиворечивую дедуктику. Мы покажем, что это невозможно, ссылаясь на критерий, установленный в предыдущем параграфе.

Итак, нам надо показать, что существует такое неперечислимое множество натуральных чисел, принадлежность к которому выразима посредством только что введенной фундаментальной пары $\langle A, T\rangle$. С этой целью мы введем в рассмотрение некоторый класс множеств, принадлежность к которым заведомо выразима посредством $\langle \Lambda, T\rangle$, а затем попытаемся установить наличие в этом классе неперечислимого множества. Класс, о котором идет речь, — класс так называемых арифметических множеств — вводится следующим образом.

Пусть α — формула, не имеющая параметров, кроме, быть может, переменной x_1. Тогда для каждой цифры n формула $S_n^{x_1}\alpha$ является суждением — истинным или ложным. Рассмотрим множество всех тех и только тех цифр n, для которых $S_n^{x_1}\alpha$ — истинное суждение. Будем говорить, что это множество *сопряжено* с формулой α. Каждое множество цифр (а также соответствующее множество чисел), сопряженное с некоторой формулой языка арифметики, будем называть *арифметическим по Гёделю* или, короче, просто *арифметическим.*

Арифметические множества обладают рядом очевидных свойств:

Свойство 1. Дополнение к арифметическому множеству (до натурального ряда $\mathbb{N}$) есть арифметическое множество. В самом деле, если M сопряжено с α, то $(\mathbb{N} \setminus M)$ сопряжено с $\neg\alpha$.

Свойство 2. Объединение и пересечение арифметических множеств суть арифметические множества. В самом деле, если M_1 и M_2 сопряжены с α_1 и α_2, то $M_1 \cap M_2$ сопряжено с $(\alpha_1 \wedge \alpha_2)$, а $M_1 \cup M_2$ — с $(\alpha_1 \vee \alpha_2)$.

Свойство 3. Принадлежность к произвольному арифметическому множеству выразима посредством $\langle A, T\rangle$. В самом деле, пусть множество M сопряжено с формулой α. Определим функцию f следующим образом: значение f на цифре n есть слово $S_n^{x_1}\alpha$. Тогда f будет вычислимой функцией, выражающей принадлежность к множеству M.

Ключевым пунктом излагаемого нами доказательства теоремы Гёделя является следующее утверждение:

(*) *существует неперечислимое арифметическое множество.*

Обоснование этого утверждения (*) мы отложим до следующего параграфа. А сейчас заметим, что из него в силу свойства 3 и теоремы 5 вытекает, что

для фундаментальной пары $\langle A, T\rangle$ языка арифметики нельзя ввести полной непротиворечивой дедуктики.

Этот результат может быть назван теоремой Гёделя о неполноте для формальной арифметики. Он показывает, что для любого точно сформулированного понятия доказательства найдется либо доказуемое, но ложное утверждение, формулируемое на языке арифметики, либо истинное утверждение того же языка, не являющееся доказуемым.

Замечание 1. Пусть M — неперечислимое арифметическое множество. Как гласит вторая часть теоремы 5, не существует дедуктики, одновременно непротиворечивой и полной применительно к множеству V значений произвольной вычислимой функции f выражающей принадлежность к M. Таким образом, для непротиворечивой дедуктики уже среди членов последовательности $f(0)$, $f(1)$, $f(2)$, ... непременно встретятся истинные, но не доказуемые утверждения

В качестве f, как мы только что видели, можно взять функцию $n \longmapsto S_n^{x_1}\alpha$, где M сопряжено с α. При таком выборе f слово $f(n)$ естественно интерпретируется как утверждение «$n \in M$». Поэтому, говоря неформально, истинное недоказуемое утверждение можно найти (для любой непротиворечивой дедуктики!) среди утверждений вида «$n \in M$». В следующем параграфе мы увидим, что M может быть выбрано так, что его дополнение E до натурального ряда $\mathbb{N}$ окажется перечислимым. Итак, существует такое перечислимое множество E, что среди истинных утверждений вида «n не принадлежит E» для любой непротиворечивой дедуктики найдется недоказуемое (заменить в этой формулировке «n не принадлежит E» на «n принадлежит E» было бы ввиду теоремы 1 невозможно).

Замечание 2. Многие определения в этом параграфе используют индукцию по построению термов и формул. При этом возникает следующая трудность: представим себе, например, что слово X имеет вид $(\alpha \wedge \beta)$ и одновременно имеет вид $(\alpha' \to \beta')$, где α, β, α', β' — некоторые формулы. В этом случае требования пунктов индуктивного определения, касающихся формул вида $(\alpha \wedge \beta)$ и формул вида $(\alpha' \to \beta')$, могут противоречить друг другу.

Поэтому, давая индуктивные определения, мы должны быть уверены в однозначности анализа термов и формул, т. е. в том, что указанные в определении терма (или формулы) случаи исключают друг друга и что в тех из них, в которых терм или формула получается в результате комбинации двух термов или формул, комбинируемые термы или формулы восстанавливаются однозначно. Именно для этой цели в формулах употребляются скобки [1]). Для формального доказательства однозначности анализа полезно следующее вспомогательное утверждение:

---

[1]) В естественном языке похожую роль играют знаки препинания. Постановка запятой в известной фразе «казнить нельзя помиловать» есть фактически выбор между «казнить $\wedge$ нельзя помиловать» и «казнить нельзя $\wedge$ помиловать». Впрочем, иногда двусмысленность не может быть устранена расстановкой знаков препинания: в фразе «Он из Германии туманной привез учености плоды» эпитет «туманной» можно отнести и к Германии, и (что менее очевидно) к учености.

число открывающихся скобок в терме или формуле равно числу закрывающихся; если слово X является началом терма или формулы, не совпадающим со всем термом или со всей формулой, то число открывающихся скобок в X больше числа закрывающихся.

§ 5. ТРИ АКСИОМЫ ТЕОРИИ АЛГОРИТМОВ

5.0. Наша цель теперь — доказать утверждение (*) из предыдущего параграфа. Однако наших расплывчатых представлений об алгоритмах, которыми мы довольствовались до сих пор, недостаточно для этой цели. Традиционный путь состоит в том, чтобы обратиться к одному из так называемых «уточнений» понятия алгоритма, т. е. заменить несколько неопределенное, но зато совершенно общее понятие алгоритма, которым мы все время пользовались, достаточно точным, но зато и более узким, понятием «алгоритма специального вида»[1]). Об одном из таких понятий «алгоритмов специального вида» рассказано в брошюре автора «Машина Поста» (М.: Наука, 1979); о другом см. далее в приложении В. Здесь мы, однако, изберем другой путь: не привязывая изложения к тому или иному специальному классу алгоритмов, мы вместо этого попытаемся сформулировать некоторые ограничения, налагаемые на наши первоначальные представления об алгоритмах. Эти ограничения будут сформулированы в виде трех аксиом: аксиомы протокола, аксиомы программы и аксиомы арифметичности.

5.1. Первая аксиома. Рассмотрим процесс применения какого-либо алгоритма A к исходному

---

[1]) Это более узкое понятие провозглашается, впрочем, равносильным первоначальному, широкому, в том точном смысле, что классы вычислимых функций, возникающие на базе каждого из этих понятий, совпадают (а следовательно, совпадают и классы перечислимых множеств). Указанное совпадение воспринимается не как теорема, подлежащая доказательству, а как гипотеза, проверяемая на практике. После этого строится точная математическая теория функций, вычисляемых «алгоритмами специального вида» (технически наиболее сложным при этом оказывается доказательство утверждений, аналогичных утверждениям задач 9 и 10 к приложению В). Недоказываемая догма о совпадении классов таких функций с классом всех вычислимых функций служит лишь для обоснования значимости построенной теории.

данному x с получением результата y. Мы предполагаем, что все промежуточные выкладки, весь процесс вычисления[1]), ведущий от x к y, можно запротоколировать так, чтобы этот протокол содержал исчерпывающую информацию о последовательных этапах процесса.

Пример 1. При работе вычислительной машины, в целях проверки ее работы, часто бывает нужно выдать наружу, «на печать», не только конечный результат, но и все промежуточные результаты. Получаемый таким способом «протокол работы машины» будет словом в выходном алфавите машины — с добавлением, если нужно, знака пробела, знака новой строки и т. п.

Пример 2. Желая проверить, правильно ли усвоен обучающимися алгоритм сложения чисел столбиком, мы можем требовать, чтобы в своих письменных работах они не только указывали конечный результат, но и записывали в определенной системе записи все свои действия. Можно договориться о такой системе записи вычислений, чтобы для сложения, например, чисел 68 и 9967 протокол выглядел так:

		1	11	111	1111	1111	
68, 9967	68	68	68	68	68	68	10035
	9967	9967	9967	9967	9967	9967	
		5	35	035	0035	10035	

Каждый из образующих протокол членов есть либо число в десятичной системе (в нашем примере 10035), либо пара чисел (в нашем примере 68, 9967), либо, наконец, четырехэтажное образование вида

11
68
9967
35

(«подвальный» и «чердачный» этажи могут быть и пустыми). Не представляет труда оформить протокол в виде слова в некотором алфавите. Для этого достаточно ввести некоторые дополнительные знаки, с

[1]) Слово «вычисление» понимается здесь в самом широком смысле, отнюдь не исчерпывающемся обычными «цифровыми» подсчетами.

тем чтобы только что изображенный четырехэтажный объект записать прежде в виде таблицы

*	*	1	1	*
*	*	*	6	8
*	9	9	6	7
*	*	*	3	5

а затем в виде слова (**11*/***68/*9967/***35). А весь протокол сложения 68 и 9967 запишем так:

(68 + 9967) (*****/***68/*9967/*****) (***1*/***68/*9967/****5) (**11*/***68/*9967/***35) (*111*/***68/*9967/**035) (1111*/***68/*9967/*0035) (1111*/***68/*9967/10035) (10035).

При такой системе записи протокол сложения любых двух чисел является словом в 15-буквенном алфавите {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, (,), /, +, *}.

Эти примеры подводят нас к следующим соображениям общего характера. Мы предполагаем, что:

1) для каждого алгоритма **A** имеется некоторый алфавит Π_0 (алфавит протоколов) и всевозможные протоколы, фиксирующие работу **A** при различных исходных данных из его области применимости, образуют подмножество P_0 множества Π_0^∞;

2) существуют такие вычислимые функции α и ω, что для каждого протокола p_0 из P_0 значениями $\alpha(p_0)$ и $\omega(p_0)$ служат соответственно то исходное данное x и тот результат y, для которых составлен данный протокол (т. е. для которых протоколируется переработка x в y);

3) P_0 разрешимо относительно Π_0^∞.

Переформулируем сказанное короче, в виде следующей аксиомы, которую и будем называть *аксиомой протокола*:

для каждого алгоритма **A** *существуют алфавит* Π_0, *разрешимое подмножество* P_0 *множества* Π_0^∞, *вычислимая функция* α *и вычислимая функция* ω, *обладающие следующим свойством:*

$A(x)=y$ тогда и только тогда, когда существует такое p_0 из P_0, что $\alpha(p_0)=x$ и $\omega(p_0)=y$.

Эта аксиома имеет непосредственное

Следствие 1. *Область применимости и множество результатов любого алгоритма перечислимы.*

Доказательство. Первое из этих множеств есть $\alpha(P_0)$, а второе — $\omega(P_0)$; оба эти множества перечислимы ввиду лемм 2 и 4 и примера 2 из § 2.

Следствие 2 (из следствия 1). *Область определения и множество значений любой вычислимой функции перечислимы.*

Следствие 3. *График произвольной вычислимой функции (т. е. множество всех таких пар $\langle x, y\rangle$, что $f(x)=y$) есть перечислимое множество.*

Доказательство. Применяем аксиому протокола к алгоритму, вычисляющему f, и берем соответствующие множество P_0, функции α и ω. Строим вычислимую функцию ψ, полагая $\psi(p)=\langle\alpha(p), \omega(p)\rangle$. Замечаем, что график функции f совпадает с множеством $\psi(P_0)$, и применяем лемму 4.

Замечание 1. Следствие 2 можно было бы получить из следствия 3, с учетом следствия 2 леммы 4 и того, что область определения функции и множество значений функции представляются соответственно в виде $\text{пр}_1 M$ и $\text{пр}_2 M$, где M — график функции.

Замечание 2. Перечислимость графика есть не только необходимое (как это устанавливается следствием 3), но и достаточное условие вычислимости функции. В самом деле, если график пуст, функция нигде не определена и потому вычислима. Если же график функции f не пуст и перечисляется вычислимой функцией ψ, то предлагается такой алгоритм, вычисляющий функцию f: для того чтобы вычислить значение $f(a)$, перебирай пары $\psi(0)$, $\psi(1)$, $\psi(2)$, ... до тех пор, пока не получишь пары с первым членом a; второй член этой пары и есть $f(a)$.

5.2. Вторая аксиома. Функции, аргументы которых лежат в X, а значения — в Y, принято называть функциями *из X в Y*. Аналогично алгоритмы, у которых возможные исходные данные лежат в X, а результаты — в Y, будем называть алгоритмами *из X в Y*; в этом случае мы принимаем, что $X=\text{К}^\infty$, $Y=\text{Л}^\infty$, где К и Л — некоторые алфавиты. Каждый алгоритм из К^∞ в Л^∞ есть предписание, т. е. текст на русском

или каком-либо другом (в частности, искусственном, специально созданном для записи алгоритмов) языке. Хотя в конкретных случаях обычно не возникает сомнений, является или нет данный текст алгоритмом, само понятие предписания слишком неопределенно для того, чтобы мы могли недвусмысленно отличать предписания от непредписаний. Кроме того, у нас нет единого и достаточно точного способа понимать предписания — ведь они могут быть написаны на разных языках, да и в пределах одного языка проблема смысла достаточно сложна. Тем не менее мы предполагаем (и это предположение и составит аксиому программы), что можно выделить четко очерченное множество единообразно понимаемых предписаний (называемых *программами*), причем такое множество, которое было бы представительным в уточняемом ниже смысле. Два алгоритма назовем *равносильными*, коль скоро у них совпадают области применимости и для любого объекта из этой области, взятого в качестве исходного данного, совпадают результаты обоих алгоритмов. Множество алгоритмов из $К^\infty$ в $Л^\infty$ назовем *представительным* (для алфавитов К и Л), коль скоро любой алгоритм из $К^\infty$ в $Л^\infty$ равносилен некоторому алгоритму из рассматриваемого множества. Под «четко очерченным» множеством будем понимать здесь разрешимое подмножество множества всех слов в некотором алфавите. Под «единообразным пониманием» разумеем наличие алгоритма U, применяемого к парам ⟨программа p, исходное данное a⟩ и дающего в качестве своего результата результат применения программы p к исходному данному a.

Замечание 3. К такой схеме легко сводятся упоминавшиеся уже «уточнения» понятия алгоритма. Каждое такое уточнение состоит, по существу, в том, что указывается некоторое множество P_1 программ, некоторый неформальный алгоритм U, объясняющий, как применяется программа к заданному исходному объекту; затем провозглашается (в качестве недоказываемой догмы) представительность множества P_1.

Итак, мы предполагаем, что:

1) для каждых двух алфавитов К и Л имеется некоторый алфавит $П_1$ (алфавит программ) и некоторое множество алгоритмов P_1, называемых программами и записанных в алфавите $П_1$ (так что $P_1 \subseteq П_1^\infty$);

2) существует алгоритм $\boldsymbol{U}$ из $\Pi_1^\infty \times К^\infty$ в $Л^\infty$ (алгоритм применения программы) такой, что $\boldsymbol{U}(p, a)$ есть результат применения p к a;

3) множество P_1 является представительным;

4) множество P_1 разрешимо относительно Π_1^∞.

При этом вовсе не предполагается, что алфавит Π_1, множество P_1 и алгоритм $\boldsymbol{U}$ могут быть выбраны лишь единственным образом. Всякую тройку $\langle \Pi_1, P_1, \boldsymbol{U} \rangle$, где Π_1 — алфавит, P_1 — множество всех программ, записанных в этом алфавите, и $\boldsymbol{U}$ — алгоритм применения программы к аргументу, будем называть *способом программирования из* $К^\infty$ *в* $Л^\infty$.

Таким образом, при заданных К и Л возможны различные способы программирования.

Замечание 4. Предположения 1)—4) вовсе не определяют понятия «способ программирования» (это понятие остается понимаемым интуитивно), а лишь указывают некоторые (причем, как показывает более глубокий анализ, еще не все) его свойства и постулируют, что тройка с такими свойствами существует.

Переходим теперь к формулировке второй аксиомы. Но сначала одно обозначение. Пусть $\boldsymbol{G}$ — произвольный алгоритм из $\Pi_1^\infty \times К^\infty$ в $Л^\infty$. Через $\boldsymbol{G}_p$, где $p \in \Pi_1^\infty$, обозначим следующий алгоритм из $К^\infty$ в $Л^\infty$: для любого a из $К^\infty$ в качестве результата применения $\boldsymbol{G}_p$ к a берем результат применения $\boldsymbol{G}$ к паре $\langle p, a \rangle$ [так что $\boldsymbol{G}_p(a) \simeq \boldsymbol{G}(p, a)$]. С помощью этого обозначения мы можем переформулировать предположения 1)—4) в виде следующей *аксиомы программы*:

для любых двух алфавитов К *и* Л *существуют алфавит* Π_1, *разрешимое подмножество* P_1 *множества* Π_1^∞ *и алгоритм* $\boldsymbol{U}$ *из* $\Pi_1^\infty \times К^\infty$ *в* $Л^\infty$, *обладающие следующими свойствами: для всякого алгоритма* $\boldsymbol{A}$ *из* $К^\infty$ *в* $Л^\infty$ *найдется такое* p *из* P_1, *что алгоритмы* $\boldsymbol{A}$ *и* $\boldsymbol{U}_p$ *равносильны.*

Эта аксиома также имеет важные следствия. Но прежде ряд определений.

Пусть I, X и Y — некоторые множества, F — функция из $I \times X$ в Y. Если i — элемент множества I, то через F_i мы будем обозначать функцию из X в Y, которая определена на тех x, для которых пара $\langle i, x \rangle$ лежит в области определения функции F; в этом слу-

чае значение F_i на x равно $F(i, x)$. С помощью знака условного равенства сказанное можно записать короче: $F_i(x) \simeq F(i, x)$.

Пусть теперь Φ — некоторый класс функций из X в Y; функцию F из $I \times X$ в Y назовем *универсальной* для класса Φ, если выполнены следующие два условия:

1° при всяком $i \in I$ функция F_i принадлежит классу Φ;

2° всякая функция из Φ есть F_i при некотором i; иными словами, для всякой $\varphi \in \Phi$ существует такое $i \in I$, что для всех $x \in X$ верно условное равенство $\varphi(x) \simeq F(i, x)$.

Следствие 1 аксиомы программы. *Пусть* К *и* Л — *два алфавита*, Φ — *семейство всех вычислимых функций из* $К^{\infty}$ *в* $Л^{\infty}$. *Тогда существует вычислимая функция из* $\mathbb{N} \times К^{\infty}$ *в* $Л^{\infty}$, *универсальная для класса* Φ.

Доказательство. Условие 1 выполнено автоматически для любой вычислимой функции F (если F вычислима, то и все F_i вычислимы). Поэтому достаточно построить вычислимую функцию F из $\mathbb{N} \times К^{\infty}$ в $Л^{\infty}$, удовлетворяющую условию 2. Рассмотрим алфавит $П_1$, разрешимое подмножество P_1 множества $П_1^{\infty}$ и алгоритм $\boldsymbol{U}$ из $П_1^{\infty} \times К^{\infty}$ в $Л^{\infty}$, существующие по аксиоме программы. Будучи разрешимым подмножеством перечислимого множества, множество P_1 перечислимо (лемма 2); пусть f — перечисляющая его функция. Тогда функция F, определенная соотношением

$$F(i, x) \simeq \boldsymbol{U}(f(i), x),$$

будет искомой. В самом деле, пусть φ — любая вычислимая функция из $К^{\infty}$ в $Л^{\infty}$, $\boldsymbol{A}$ — вычисляющий ее алгоритм: $\boldsymbol{A}(x) \simeq \varphi(x)$ для всех $x \in К^{\infty}$. В силу аксиомы программы существует такое p из P_1, что для всех $x \in К^{\infty}$ выполнено условное равенство

$$\boldsymbol{U}(p, x) \simeq \boldsymbol{A}(x).$$

Так как $p \in P_1$, то $p = f(i)$ при некотором i; для этого i имеет место цепочка условных равенств

$$F(i, x) \simeq \boldsymbol{U}(f(i), x) \simeq \boldsymbol{U}(p, x) \simeq \boldsymbol{A}(x) \simeq \varphi(x),$$

показывающая, что для построенной нами функции F выполнено условие 2° определения универсальной функции.

Частным случаем следствия 1 является

Следствие 2. *Существует вычислимая функция F из $\mathbb{N}\times\mathbb{N}$ в $\mathbb{N}$, универсальная для класса всех вычислимых функций из $\mathbb{N}$ в $\mathbb{N}$.*

Следствие 2 получается из следствия 1, если взять в качестве К и Л один из цифровых алфавитов для записи чисел, например алфавит $\{|\}$.

Будем говорить, что функции f и g из X в Y всюду отличаются, если ни при каком x из X условное равенство $f(x)\simeq g(x)$ не имеет места (это означает, что для всякого x хотя бы одна из функций f и g определена на x и что если обе функции определены на x, то их значения различны).

Следствие 3 (из следствия 2). *Существует такая вычислимая функция d из $\mathbb{N}$ в $\mathbb{N}$, что никакая вычислимая функция из $\mathbb{N}$ в $\mathbb{N}$ не может отличаться от нее всюду.*

Доказательство. Пусть F — универсальная функция из следствия 2. Возьмем в качестве d функцию, определяемую соотношением

$$d(i)\simeq F(i, i).$$

В этом случае $d(i)\simeq F_i(i)$, поэтому d и F_i не могут отличаться всюду; так как любая вычислимая функция из $\mathbb{N}$ в $\mathbb{N}$ есть F_i при некотором i, то никакая вычислимая функция из $\mathbb{N}$ в $\mathbb{N}$ не может всюду отличаться от d.

Это следствие может поначалу показаться парадоксальным: казалось бы, функция $d_1(x)\simeq d(x)+1$ всюду отличается от d. Разрешение кажущегося противоречия состоит в том, что d — не всюду определенная функция, и на тех x, на которых d не определена, d_1 не определена тоже, и для этих x условное равенство $d_1(x)\simeq d(x)$ выполнено. Однако мы можем рассмотреть не саму функцию d_1, а какое-нибудь всюду определенное продолжение D_1 функции d_1 (это значит, что D_1 — всюду определенная функция, совпадающая с d_1 там, где d_1 определена). Теперь уже D_1 всюду отличается от d: если $d(x)$ определено, то $d_1(x)$ также определено и равно $d(x)+1$, поэтому $D_1(x)=d(x)+1\not\simeq d(x)$; если же $d(x)$ не определено, то $D_1(x)\not\simeq$

$\not\simeq d(x)$ уже потому, что левая часть этого соотношения определена, а правая — нет. Не вошли ли мы в противоречие со следствием 3? Нет — мы доказали только, что никакое всюду определенное продолжение функции d_1 не может быть вычислимым, получив тем самым

Следствие 4 (из следствия 3). *Существует вычислимая функция с натуральными аргументами и значениями, не имеющая всюду определенного вычислимого продолжения.*

Пусть q — вычислимая функция с натуральными аргументами и значениями, не имеющая всюду определенного вычислимого продолжения; может ли область определения q быть разрешимым подмножеством $\mathbb{N}$? Легко понять, что нет: в самом деле. если бы она была разрешимым подмножеством $\mathbb{N}$, то функция Q, определяемая равенством

$$Q(x) = \begin{cases} q(x), & \text{если } x \text{ принадлежит области определения } q, \\ 0, & \text{если } x \text{ не принадлежит области определения } q, \end{cases}$$

была бы вычислимым всюду определенным продолжением q. Итак, область определения функции q — неразрешимое множество; согласно следствию 2 аксиомы протокола это множество перечислимо. Таким образом, нами доказано

Следствие 5 (из следствия 4). *Существует перечислимое неразрешимое подмножество натурального ряда.*

Факт существования перечислимого неразрешимого подмножества натурального ряда — один из важнейших фактов теории алгоритмов. Так как подмножество натурального ряда разрешимо тогда и только тогда, когда оно и его дополнение перечислимы (лемма 3), то предыдущее следствие может быть переформулировано так:

Следствие 6 (из следствия 5). *Существует перечислимое подмножество натурального ряда с неперечислимым дополнением.*

5.3. Третья аксиома. Если отвлечься от того (впрочем, весьма существенного) обстоятельства, что на вычислительных машинах могут вычисляться лишь

функции, определенные на конечных множествах натуральных чисел (поскольку слишком большие аргументы просто не смогут поместиться в машине), то можно считать, что на этих машинах вычисляются вычислимые числовые функции. Как известно, основными операциями, совершаемыми машиной, являются сложение, умножение и логические операции. Опыт работы на машинах приводит к убеждению, что с помощью этих операций можно запрограммировать любую вычислимую функцию. Следовательно, и всякое перечислимое множество натуральных чисел (как множество значений вычислимой функции) может быть записано в терминах сложения, умножения и логических операций. Сказанное[1]) делает естественным формулировку следующей аксиомы, которую мы будем называть *аксиомой арифметичности*:

всякое перечислимое множество натуральных чисел является арифметическим.

Непосредственным следствием этой аксиомы и служит интересующее нас утверждение предыдущего параграфа:

существует арифметическое множество, не являющееся перечислимым.

Таковым является дополнение к множеству из следствия 6 п. 5.2: оно является неперечислимым множеством с перечислимым дополнением. Само это множество будет арифметическим, как дополнительное к арифметическому (1-е свойство арифметических множеств).

Таким образом, доказательство теоремы о неполноте закончено: как уже отмечалось, из существования неперечислимого арифметического множества следует существование неперечислимого множества, принадлежность которому выразима в арифметике; отсюда следует, что не существует непротиворечивой и полной дедуктики для $\langle A, T\rangle$ применительно к некоторому перечислимому подмножеству V и, следовательно, никакая непротиворечивая дедуктика не может быть полной для $\langle A, T\rangle$.

---

[1]) Более подробно эти соображения будут развиты в приложении В.

ПРИЛОЖЕНИЯ

А. СИНТАКСИЧЕСКАЯ И СЕМАНТИЧЕСКАЯ ФОРМУЛИРОВКИ ТЕОРЕМЫ О НЕПОЛНОТЕ

1. Постановка задачи. Доказанную нами формулировку теоремы Гёделя естественно называть семантической, так как в ней шла речь об истинности суждений арифметики. Вообще, семантикой называется та часть науки о языке (языке арифметики в нашем случае), которая интересуется смыслом выражений, их истинностью и ложностью, — в отличие от синтаксиса, который изучает выражения языка как комбинации знаков, в отрыве от их смысла[1]). Мы хотим перейти к синтаксической формулировке теоремы о неполноте, т. е. устранить по возможности упоминания об истинности суждений.

Полностью удовлетворительное решение этой задачи требует конкретизации понятия доказательства, выходящей за рамки этой брошюры; тем не менее мы сделаем некоторые шаги в этом направлении.

2. Синтаксическая непротиворечивость и синтаксическая полнота. Пусть $\langle Д, D, \delta\rangle$ — дедуктика над алфавитом А языка арифметики. (В этом приложении мы будем рассматривать только дедуктики над А, не оговаривая этого специально.) Назовем ее *синтаксически непротиворечивой*, если не существует такого суждения α, для которого и α, и $\neg\alpha$ доказуемы в этой дедуктике. Назовем ее *синтаксической полной*, если для всякого суждения α хотя бы одно из суждений α и $\neg\alpha$ доказуемо в этой дедуктике. Эти определения

[1]) Иногда слово «синтаксис» употребляют в более узком смысле, обозначая им часть грамматики, изучающую сочетания слов в предложениях естественного языка.

можно сформулировать короче, введя предварительно понятие суждения, опровержимого в данной дедуктике, — такого суждения α, что суждение $\neg\alpha$ доказуемо в ней. Теперь можно сказать так: дедуктика синтаксически непротиворечива, если никакое суждение не является доказуемым и опровержимым одновременно, и синтаксически полна, если всякое суждение либо доказуемо, либо опровержимо.

Следующая лемма устанавливает связь между этими понятиями и понятиями непротиворечивой и полной (относительно $\langle A, T\rangle$) дедуктики. Напомним, что дедуктика называется непротиворечивой, если все доказуемые суждения истинны, и полной, если все истинные суждения доказуемы.

Лемма А.1. А) *Непротиворечивая дедуктика синтаксически непротиворечива.*

Б) *Полная дедуктика синтаксически полна.*

В) *Если дедуктика непротиворечива, то полнота ее равносильна синтаксической полноте.*

Доказательство. А) Если α и $\neg\alpha$ доказуемы в непротиворечивой дедуктике, то α и $\neg\alpha$ истинны, что противоречит определению истинности. Б) Одно из суждений α и $\neg\alpha$ должно быть истинным, а следовательно, и доказуемым, если дедуктика полна. В) Если α — истинное суждение, то $\neg\alpha$ — ложное, поэтому $\neg\alpha$ не может быть доказуемо в непротиворечивой дедуктике и — если дедуктика синтаксически полна — α должно быть доказуемым.

Учитывая лемму, естественно предложить в качестве синтаксического варианта теоремы о неполноте такое утверждение:

не существует синтаксически непротиворечивой и синтаксически полной дедуктики для языка арифметики.

Этот вариант хорош тем, что, во-первых, из него вытекает доказанный нами семантический вариант теоремы о неполноте и, во-вторых, тем, что в нем совсем ничего не говорится об истинности. Однако так сформулированное утверждение неверно — дедуктика, в которой доказуемы те и только те суждения, в которые четное число раз входит символ $\neg$ (такая существует в силу теоремы 1), будет синтаксически непротиворечива и синтаксически полна. Поразмыслив о постигшей нас неудаче, мы приходим к выводу, что

причина ее как раз в том, что рассмотренная формулировка никак не связана с обычным пониманием знаков алфавита A — в построенной дедуктике одновременно доказуемы, например, формулы $(2\cdot 2)=4$ и $(2\cdot 2)=5$. Мы выйдем из создавшегося положения, потребовав от дедуктики, чтобы некоторые суждения обязательно были доказуемыми в ней. Уточним сказанное.

Пусть D_0, D — некоторые дедуктики. Будем говорить, что D является *расширением* D_0, если всякое суждение, доказуемое в D_0, доказуемо и в D. (В этом случае, очевидно, всякое опровержимое в D_0 суждение опровержимо и в D.) Будем говорить, что дедуктика D_0 *пополнима*, если существует ее *пополнение*, т. е. расширение, являющееся синтаксически непротиворечивой и синтаксически полной дедуктикой. Приведенный выше пример устанавливает пополнимость пустой дедуктики — дедуктики, в которой ни одно утверждение не доказумо. Используя понятие пополнимости, мы можем предложить в качестве синтаксического варианта теоремы Гёделя такое утверждение:

существует непополнимая дедуктика.

Однако это утверждение бессодержательно, так как всякая синтаксически противоречивая дедуктика непополнима. Кроме того, нам хотелось бы, чтобы из синтаксического варианта теоремы о неполноте вытекал доказанный нами семантический вариант. Мы удовлетворим этому требованию, выбрав такую формулировку:

существует непротиворечивая непополнимая дедуктика.

(Отсюда следует несуществование полной непротиворечивой дедуктики, так как такая дедуктика являлась бы пополнением любой непротиворечивой.) На этой формулировке мы и остановимся. Но прежде чем доказывать сформулированное утверждение, объясним, чем оно лучше исходной семантической формулировки, — ведь в нем мы говорим о непротиворечивости, определение которой апеллирует к истинности. Дело в том, что непротиворечивую непополнимую дедуктику можно указать явно и утверждение о непополнимости этой явно заданной дедуктики уже никак не апеллирует к понятию истинности. (Конечно, ценность этого утверждения в наших глазах определяется нашей

верой в непротиворечивость этой дедуктики.) Перейдем теперь к доказательству сформулированного утверждения. Для этого нам понадобятся некоторые новые понятия из теории алгоритмов.

3. **Неотделимые множества.** Пусть К — алфавит, A и B — непересекающиеся подмножества $К^\infty$. Будем говорить, что множество C *отделяет* A от B, если $A \subset C$ и $B \cap C = \varnothing$. Если множество C отделяет A от B, то его дополнение (до $К^\infty$) отделяет B от A. Будем говорить, что A и B *отделимы*, если существует разрешимое подмножество C множества $К^\infty$, отделяющее A от B. (В этом случае дополнение C является разрешимым подмножеством $К^\infty$, отделяющим B от A.)

Лемма А.2. *Непересекающиеся множества A и B отделимы тогда и только тогда, когда функция из $К^\infty$ в $\mathbb{N}$, определенная соотношением*

$$f(x)=\begin{cases} 1, & \text{если } x \in A, \\ 0, & \text{если } x \in B, \\ \text{не определена}, & \text{если } x \notin A \cup B, \end{cases}$$

имеет всюду определенное вычислимое продолжение.

Доказательство. Если g — всюду определенное вычислимое продолжение f, то разрешимое множество $\{x \mid g(x) = 1\}$ отделяет A от B. Наоборот, если разрешимое множество C отделяет A от B, то вычислимая функция g, равная 1 на элементах C и 0 вне C, продолжает f.

Лемма А.3. *Существуют перечислимые неотделимые подмножества* $\mathbb{N}$.

Доказательство. Согласно предыдущей лемме достаточно доказать, что существует вычислимая функция h из $\mathbb{N}$ в $\mathbb{N}$, принимающая лишь два значения — 0 и 1 — и не имеющая всюду определенного вычислимого продолжения. В этом случае перечислимые (согласно лемме 6 и следствию 1 аксиомы протокола) множества $\{x \mid h(x) = 1\}$ и $\{x \mid h(x) = 0\}$ будут неотделимы. Чтобы построить функцию h с указанными свойствами, рассмотрим (следуя доказательству следствия 4 аксиомы программы в § 5) функцию d, от которой никакая вычислимая функция не может

отличаться всюду. Функцию h определим так:

$$h(x)=\begin{cases} 1, & \text{если } d(x)=0, \\ 0, & \text{если } d(x) \text{ определено} \\ & \text{и не равно } 0, \\ \text{не определено}, & \text{если } d(x) \text{ не определено.} \end{cases}$$

Всякое всюду определенное продолжение функции h всюду отличается от d, поэтому не может быть вычислимым.

С помощью понятия неотделимости мы сформулируем признак непополнимости дедуктики.

Теорема А.1. *Если множества доказуемых и опровержимых в данной дедуктике суждений неотделимы, то эта дедуктика непополнима.*

Доказательство. Если эта дедуктика имеет пополнение, то множества доказуемых и опровержимых в этом пополнении суждений — непересекающиеся перечислимые множества, дающие в объединении множество всех суждений. В силу леммы 3 каждое из них, в частности, множество S доказуемых суждений, является разрешимым подмножеством множества всех суждений и, следовательно, разрешимым подмножеством множества A^{∞}. Множество S отделяет множество доказуемых в исходной дедуктике суждений от множества суждений, опровержимых в ней, что противоречит предположению.

4. Построение непополнимой дедуктики. Мы построим непополнимую дедуктику, применяя теорему А.1. Пусть P и Q — перечислимые неотделимые подмножества $\mathbb{N}$ (их существование установлено в лемме А.3). Множество P арифметично по аксиоме арифметичности (§ 5); пусть α — формула, с которой оно сопряжено. Обозначим через $[n \in P]$ формулу $S_n^{x_1}\alpha$ (n — цифра); формула $[n \in P]$ истинна тогда и только тогда, когда $n \in P$. Для каждого n из P рассмотрим (истинную) формулу $[n \in P]$; для каждого n из Q рассмотрим (также истинную) формулу $\neg[n \in P]$. Рассмотренные формулы образуют перечислимое множество. Согласно теореме 1 существует дедуктика, в которой доказуемы эти формулы и только они. Эта дедуктика непротиворечива. Докажем, что она непополнима. Согласно теореме А.1 для этого

достаточно доказать, что множества доказуемых и опровержимых в ней формул неотделимы; покажем это. Если $n \in P$, то формула $[n \in P]$ доказуема, если $n \in Q$, то формула $[n \in P]$ опровержима. Поэтому, если бы разрешимое множество S отделяло доказуемые формулы от опровержимых, то разрешимое множество $\{n \mid [n \in P] \in S\}$ отделяло бы P от Q, что невозможно. Итак, непополнимая дедуктика построена.

Б. АРИФМЕТИЧЕСКИЕ МНОЖЕСТВА И ТЕОРЕМА ТАРСКОГО О НЕАРИФМЕТИЧНОСТИ МНОЖЕСТВА ИСТИННЫХ ФОРМУЛ ЯЗЫКА АРИФМЕТИКИ

Как объяснялось в § 4, суждения языка арифметики являются высказываниями о свойствах натурального ряда и операций сложения и умножения. Они бывают истинными и ложными. Для формулы с параметрами вопрос «истинна она или ложна?» лишен смысла. Если мы вместо параметров формулы подставим цифры, то получим суждение, истинность которого зависит от того, какие именно цифры мы подставили. Таким образом, формулы с параметром можно интерпретировать как свойства натуральных чисел.

Пример 1. Результат подстановки n вместо x_1 в формулу $\exists x_2((x_2 + x_2) = x_1)$ является истинным суждением тогда и только тогда, когда n четно. Поэтому можно сказать, что эта формула выражает свойство «x_1 четно». Говорят также (не вполне корректно), что эта формула истинна при четных значениях x_1 и ложна при нечетных значениях x_1.

Пример 2. Формула

$$\exists x_3 ((x_1 + x_3) = x_2)$$

выражает свойство «$x_1 \leqslant x_2$».

Пример 3. Формула

$$\exists x_2 ((x_1 \cdot x_2) = x_3)$$

выражает свойство «x_1 делит x_3».

Пример 4. Обозначим формулу из примера 3 через $[x_1 \text{ делит } x_3]$. Тогда формула

$$\forall x_1 ([x_1 \text{ делит } x_3] \to ((x_1 = 1) \vee (x_1 = x_3)))$$

выражает свойство «x_3 — простое или $x_3 = 1$».

Пример 5. Обозначим формулу из примера 1 через [x_1 четно]. Тогда формула

$$\forall x_1([x_1 \text{ делит } x_3] \rightarrow ([x_1 \text{ четно}] \vee (x_1 = 1)))$$

выражает свойство «всякий делитель x_3 или четен, или равен 1», т. е. свойство «x_3 есть степень числа 2».

Свойства, выражаемые формулами языка арифметики, назовем арифметическими. Отождествляя свойство с множеством удовлетворяющих ему объектов, приходим к определению арифметического подмножества $\mathbb{N}^k$, частным случаем которого (при $k = 1$) будет данное в § 4 определение арифметических подмножеств $\mathbb{N}$.

Дадим точные определения. Пусть α — формула языка арифметики, $w_1, \ldots, w_p$ — переменные, $c_1, \ldots$ $\ldots, c_p$ — цифры. *Результатом подстановки* $c_1, \ldots, c_p$ *вместо* $w_1, \ldots, w_p$ *в* α назовем формулу

$$S_{c_1 \ldots c_p}^{w_1 \ldots w_p}\alpha = S_{c_p}^{w_p} \ldots S_{c_2}^{w_2} S_{c_1}^{w_1}\alpha,$$

получающуюся из α последовательной подстановкой $c_1, \ldots, c_p$ вместо $w_1, \ldots, w_p$. (Нетрудно понять, что результат последовательного выполнения нескольких подстановок не зависит от порядка, так что можно было бы, например, определить $S_{c_1 \ldots c_p}^{w_1 \ldots w_p}\alpha$ как $S_{c_1}^{w_1} \ldots$ $\ldots S_{c_p}^{w_p}\alpha$ — получилось бы то же самое.) Пусть α — формула арифметики, не имеющая параметров, отличных от $x_1, \ldots, x_k$. Рассмотрим подмножество $\mathbb{N}^k$, состоящее из тех $\langle c_1, \ldots, c_k \rangle$, для которых суждение $S_{c_1 \ldots c_k}^{x_1 \ldots x_k}\alpha$ истинно. Будем говорить, что оно *сопряжено* с формулой α. Множества, сопряженные с формулами языка арифметики, будем называть *арифметическими*. При $k = 1$ мы приходим к (данному в § 4) определению арифметических подмножеств натурального ряда. Используя упоминавшееся отождествление свойств с множествами удовлетворяющих им объектов, мы будем говорить также об арифметичности свойств натуральных чисел.

Пример 6. Множества $\{\langle x_1, x_2 \rangle \mid x_1 = x_2\}$, $\{\langle x_1, x_2, x_3 \rangle \mid x_1 + x_2 = x_3\}$, $\{\langle x_1, x_2, x_3 \rangle \mid x_1 \cdot x_2 = x_3\}$ являются арифметическими, так как сопряжены с

формулами

$$x_1 = x_2, \quad (x_1 + x_2) = x_3, \quad (x_1 \cdot x_2) = x_3.$$

Пример 7. Множество $\{\langle x_1, x_2\rangle \mid x_1 \leqslant x_2\}$ сопряжено с формулой примера 2 и потому является арифметическим.

Пример 8. Множество $\{\langle x_1, x_2\rangle \mid x_1$ делит $x_2\}$ является арифметическим. Для того чтобы построить формулу, с которой оно сопряжено, нужно слегка переделать формулу из примера 3, заменив в ней x_2 на x_3 и наоборот.

Пример 9. Множество простых чисел и множество степеней числа 2 — арифметические подмножества натурального ряда. (См. примеры 4 и 5.)

Свойства арифметических подмножеств $\mathbb{N}$, указанные в § 4, остаются верными и для арифметических подмножеств $\mathbb{N}^k$. В частности, верна следующая

Лемма Б.1. а) *Дополнение к арифметическому подмножеству $\mathbb{N}^k$ (до $\mathbb{N}^k$) арифметично*;

б) *пересечение и объединение арифметических подмножеств $\mathbb{N}^k$ арифметичны.*

Следующая лемма показывает, что арифметичность сохраняется при перестановке координат.

Лемма Б.2. *Пусть σ — перестановка множества $\{1, \ldots, k\}$ (т. е. взаимно однозначное отображение его на себя), M — арифметическое подмножество $\mathbb{N}^k$. Тогда множество*

$$M^\sigma = \{\langle x_1, \ldots, x_k\rangle \mid \langle x_{\sigma(1)}, \ldots, x_{\sigma(k)}\rangle \in M\}$$

арифметично.

Доказательство. Если множество M сопряжено с формулой α, то множество M^σ сопряжено с формулой α^σ, которая получится, если в формуле α всюду заменить все переменные из списка $x_1 \ldots x_k$ на соответствующие переменные из списка $x_{\sigma(1)} \ldots \ldots x_{\sigma(k)}$.

Следующие леммы связывают классы арифметических подмножеств $\mathbb{N}^k$ при различных k.

Лемма Б.3. *Если M — арифметическое подмножество $\mathbb{N}^k$, то множество $M \times \mathbb{N}^l$ — арифметическое подмножество $\mathbb{N}^{k+l}$.*

Доказательство. В самом деле, $M \times \mathbb{N}^l$ сопряжено с той же формулой, что и M.

Лемма Б.4. *Если множество $M \subset \mathbb{N}^{k+l}$ арифметично, то его проекция M' на первые k осей, равная*

$$\{\langle x_1, \ldots, x_k\rangle \mid \exists x_{k+1} \ldots \exists x_{k+l} (\langle x_1, \ldots, x_{k+l}\rangle \in M)\},$$

является арифметическим подмножеством $\mathbb{N}^k$.

Доказательство. В самом деле, если M сопряжено с формулой α, то M' сопряжено с формулой $\exists x_{k+1} \ldots \exists x_{k+l} \alpha$.

Сочетая леммы Б.2 и Б.4, можно доказать арифметичность проекции арифметического множества на любые оси.

Пусть $M \subset \mathbb{N}^2$ — арифметическое множество. Для каждого $n \in \mathbb{N}$ рассмотрим M_n — «n-е сечение множества M», множество тех x, для которых $\langle n, x\rangle \in M$. Будучи проекцией множества $(\{n\} \times \mathbb{N}) \cap M$, оно арифметично. Назовем множество $M \subset \mathbb{N}^2$ *универсальным* арифметическим множеством, если любое арифметическое подмножество $\mathbb{N}$ является его сечением. Оказывается, такого быть не может.

Теорема Б.1. *Универсальных арифметических множеств не существует: каково бы ни было арифметическое множество $M \subset \mathbb{N}^2$, существует арифметическое множество $Q \subset \mathbb{N}$, которое отлично от всех сечений множества M.*

Доказательство. Множество $Q = \{x \mid \langle x, x\rangle \notin M\}$ арифметично, так как является проекцией множества $(\mathbb{N}^2 \setminus M) \cap \{\langle x, y\rangle \mid x = y\}$. Оно не может быть сечением M: если бы Q равнялось M_n, то по определению M_n мы имели бы $n \in Q \Longleftrightarrow \langle n, n\rangle \in M$, но по определению Q имеет место соотношение

$$n \in Q \Leftrightarrow \langle n, n\rangle \notin M.$$

(Другими словами, множества Q и M_n по-разному ведут себя по отношению к числу n, поэтому не могут совпадать.)

Назовем функцию f из $\mathbb{N}^k$ в $\mathbb{N}^l$ *арифметической*, если ее график — арифметическое подмножество $\mathbb{N}^{k+l}$.

Лемма Б.5. *Образы и прообразы арифметических множеств при арифметических функциях арифметичны.*

Доказательство. Рассмотрим, например, образ арифметического множества $A \subset \mathbb{N}$ при арифметической функции f из $\mathbb{N}$ в $\mathbb{N}$. Этот образ есть проекция множества (график f)$\cap (A \times \mathbb{N})$ и поэтому

арифметичен. Другими словами, если через $[f(x_1) = x_2]$ обозначить формулу, с которой сопряжен график f, а через $[x_1 \in A]$ — формулу, с которой сопряжено A, то формула

$$\exists x_1([f(x_1) = x_2] \wedge [x_1 \in A])$$

будет истинна для тех и только тех значений x_2, которые принадлежат образу A. Чтобы указать формулу, сопряженную с образом A, достаточно переименовать переменные (поменять всюду x_1 и x_2). Прообраз множества A при функции f будет сопряжен с формулой

$$\exists x_2([f(x_1) = x_2] \wedge [x_2 \in A]),$$

где $[x_2 \in A]$ обозначает формулу, получающуюся из $[x_1 \in A]$ переименованием переменных.

Мы стремимся доказать теорему Тарского, утверждающую, что

множество истинных формул арифметики неарифметично.

Чтобы придать смысл этой формулировке, надо объяснить, что мы имеем в виду, говоря об арифметичности множества формул — некоторого подмножества A^∞. Можно определить это понятие так: выбрать взаимно однозначное соответствие между A^∞ и $\mathbb{N}$ (*нумерацию* A^∞), сопоставляющее каждому слову X из A^∞ некоторое натуральное число (номер слова X при этой нумерации), и называть множество $M \subset \mathrm{A}^\infty$ арифметическим (относительно данной нумерации), если множество номеров слов из M является арифметическим подмножеством $\mathbb{N}$.

Конечно, это определение зависит от выбора нумерации слов алфавита A. Назовем две нумерации *арифметически эквивалентными*, если функции, дающие по номеру слова в одной из них номер того же слова в другой, арифметичны.

Лемма Б.6. *Если множество $M \subset \mathrm{A}^\infty$ арифметично относительно данной нумерации π_1, то оно арифметично относительно любой нумерации π_2, арифметически эквивалентной π_1.*

Доказательство. По условию множество $\pi_1(M)$ (состоящее из π_1-номеров слов из M) арифметично. Множество $\pi_2(M)$ является образом $\pi_1(M)$ при

арифметической (по условию) функции, дающей π_2-номера по π_1-номерам, поэтому оно также арифметично.

Окончательное определение арифметических множеств слов в алфавите А таково: *арифметическими* называются множества, арифметические относительно вычислимых нумераций множества $А^\infty$. (Нумерация называется *вычислимой*, если функция, сопоставляющая слову его номер, вычислима. В этом случае вычислима и обратная функция, сопоставляющая числу n слово с номером n; существование вычислимых нумераций $А^\infty$ установлено в примере 3 из § 2.)

Чтобы доказать корректность этого определения, достаточно показать, что все вычислимые нумерации арифметически эквивалентны. Если π_1 и π_2 — вычислимые нумерации, то функция, сопоставляющая номеру слова относительно π_1 номер того же слова относительно π_2, вычислима. (Она вычисляется следующим алгоритмом: получив аргумент x, перебирай все слова алфавита А, вычисляй их π_1-номера и жди появления слова, у которого π_1-номер равен x; найдя это слово, вычисли его π_2-номер.) Поэтому корректность будет доказана, если мы установим, что верна следующая лемма.

Лемма Б.7. *Всякая вычислимая функция из $\mathbb{N}^p$ в $\mathbb{N}^q$ арифметична.*

Доказательство. График вычислимой функции из $\mathbb{N}^p$ в $\mathbb{N}^q$ есть перечислимое подмножество $\mathbb{N}^{p+q}$ (следствие 3 аксиомы протокола), поэтому требуемое утверждение вытекает из следующей усиленной формы аксиомы арифметичности:

всякое перечислимое подмножество $\mathbb{N}^k$ арифметично.

(В § 5 аксиомой арифметичности был назван частный случай этого утверждения, возникающий при $k = 1$.)

Теорема Б.2. *Множество T истинных формул арифметики неарифметично.*

Доказательство. Покажем, что если бы T было арифметично, то в противоречии с теоремой Б.1 существовало бы универсальное арифметическое множество. Следуя Гёделю, назовем формулы, не имеющие отличных от x_1 параметров, *классовыми*. Множество всех классовых формул — разрешимое подмножество перечислимого множества $А^\infty$ и потому

перечислимо. Зафиксируем какое-нибудь вычислимое перечисление $\alpha_0, \alpha_1, \alpha_2, \ldots$ множества классовых формул. Рассмотрим множество

$$M = \{\langle n, m\rangle \mid \text{результат подстановки } m \text{ вместо } x_1 \text{ в } \alpha_n \text{ — истинное суждение}\}.$$

Очевидно, n-е сечение этого множества сопряжено с формулой α_n, а потому сечениями этого множества являются все арифметические подмножества $\mathbb{N}$. Остается показать, что если бы T было арифметично, то и M было бы арифметично. Вспоминая определение арифметичности множества слов, зафиксируем произвольную вычислимую нумерацию слов алфавита A^{∞}. Пусть T' — множество номеров слов из T при этой нумерации. Функция S, сопоставляющая паре $\langle n, m\rangle$ номер слова, являющегося результатом подстановки m вместо x_1 в α_n, вычислима и, следовательно, арифметична (лемма Б.7). Множество M является прообразом множества T' при функции S. Поэтому из арифметичности T' вытекает арифметичность M (лемма Б.5). Теорема Б.2 доказана.

Анализ доказательства теоремы Б.2 показывает, что оно связано с «парадоксом лжеца». Коротко скажем об этой связи.

Парадокс лжеца состоит в следующем. Некто заявляет: «То, что я сейчас говорю, ложно». Истинно или ложно его высказывание? Любой из ответов ведет к противоречию. Если предположить, что оно истинно, то в силу своего собственного смысла оно должно быть ложным и наоборот. Изложим теперь рассмотренное доказательство теоремы Б.2 в форме, близкой к этому парадоксу.

Пусть множество номеров истинных суждений арифметики арифметично; обозначим через [слово с номером x_3 истинно] формулу, единственным параметром которой является x_3 и которая выражает свойство «слово с номером x_3 принадлежит T», т. е. свойство «$x_3 \in T'$». Функция S арифметична; обозначим через

[x_3 есть номер результата подстановки x_2 в x_1-ю классовую формулу]

формулу, с которой сопряжен график функции S. Формула

$\exists x_3$ ([слово с номером x_3 истинно] $\wedge$

$\wedge$ [x_3 есть номер результата подстановки x_2

в x_1-ю классовую формулу])

имеет параметрами x_1 и x_2; с этой формулой сопряжено множество M; обозначим ее

[результат подстановки x_2

в x_1-ю классовую формулу истинен].

Дальше рассуждение следует доказательству теоремы о несуществовании универсального арифметического множества. Рассмотрим формулу

$\neg\exists x_2$ (($x_1 = x_2$) $\wedge$ [результат подстановки x_2

в x_1-ю классовую формулу истинен]);

обозначим ее

[результат подстановки x_1

в x_1-ю классовую формулу ложен];

она имеет параметром x_1 и отвечает своему обозначению в том смысле, что результат подстановки числа n вместо x_1 в эту формулу истинен тогда и только тогда, когда результат подстановки n в n-ю классовую формулу ложен. (Рассмотрение этой формулы соответствует рассмотрению множества Q в доказательстве теоремы Б.1.) Построенная формула является классовой и, следовательно, имеет некоторый номер (обозначим его n) в перечислении классовых формул. Подставим n вместо x_1 в построенную нами формулу, результат подстановки обозначим

[результат подстановки n

в n-ю классовую формулу ложен];

это — суждение, истинное тогда и только тогда, когда результат подстановки цифры n в n-ю классовую формулу ложен. Но этот результат представляет собой не что иное, как само рассматриваемое нами суждение. Мы получаем, что суждение

[результат подстановки n

в n-ю классовую формулу ложен]

истинно тогда и только тогда, когда ложно. (Это суждение можно было бы с полным основанием обозначить [Я ложно].) Полученное противоречие доказывает, что множество истинных формул арифметики неарифметично.

В. ЯЗЫК АДРЕСНЫХ ПРОГРАММ, РАСШИРЕННЫЙ АРИФМЕТИЧЕСКИЙ ЯЗЫК И АКСИОМА АРИФМЕТИЧНОСТИ

В этом приложении мы постараемся обосновать аксиому арифметичности. План наших рассуждений таков. Сначала мы опишем некоторый конкретный класс алгоритмов — класс адресных программ; функции, вычисляемые с помощью алгоритмов из этого класса, естественно назвать адресно вычислимыми. Затем мы докажем, что область значений всякой адресно вычислимой функции представляет собой арифметическое множество. Тем самым аксиома арифметичности будет обоснована — если поверить в то, что всякая вычислимая функция является адресно вычислимой.

Вспомогательным средством для нас будет служить расширенный арифметический язык, который отличается от описанного в § 4 языка арифметики наличием некоторых дополнительных выразительных средств. Мы покажем, что множество значений всякой адресно вычислимой функции может быть описано формулой расширенного арифметического языка. Затем мы покажем, что это расширение на самом деле несущественно и что для всякой формулы расширенного языка можно найти заменитель в обычном языке арифметики. Отсюда будет следовать, что множество значений любой адресно вычислимой функции может быть описано формулой языка арифметики, т. е. арифметично.

Начнем со следующего простого замечания: для обоснования аксиомы арифметичности и даже ее усиленного варианта, рассматриваемого и используемого в приложении Б, достаточно уметь доказывать, что

график всякой вычислимой функции из $\mathbb{N}$ *в* $\mathbb{N}$ *является арифметическим подмножеством* $\mathbb{N}^2$.

(Понятие арифметического подмножества $\mathbb{N}^2$ введено в приложении Б.) В самом деле, пусть это утверждение верно. Тогда всякое перечислимое подмножество

$\mathbb{N}$ арифметично, так как оно является проекцией графика перечисляющей его вычислимой функции (лемма Б.4). Докажем теперь усиленный вариант аксиомы арифметичности. Пусть $M \subset \mathbb{N}^k$ — перечислимое множество, g — перечисляющая его функция из $\mathbb{N}$ в $\mathbb{N}^k$. Значение функции g на числе n представляет собой кортеж из k чисел: $g(n) = \langle g_1(n), \ldots, g_k(n) \rangle$. Функции $g_1, \ldots, g_k$ суть вычислимые функции из $\mathbb{N}$ в $\mathbb{N}$, поэтому в силу сделанного нами предположения их графики арифметичны. Обозначим через $[g_i(x_1) = x_2]$ формулы, с которыми эти графики сопряжены. График g является арифметическим подмножеством $\mathbb{N}^{k+1}$, так как он сопряжен с формулой

$$[g_1(x_1) = x_2] \wedge ([g_2(x_1) = x_3] \wedge (\ldots \wedge [g_k(x_1) = x_{k+1}]) \ldots).$$

(Здесь через $[g_i(x_1) = x_{i+1}]$ обозначена формула, получающаяся из формулы $[g_i(x_1) = x_2]$ переименованием переменных, при котором переменные x_2 и x_{i+1} заменяются друг на друга.) Множество M является проекцией графика g на оси $x_2, \ldots, x_{k+1}$ и потому является арифметическим.

Итак, наша цель — доказать, что график всякой вычислимой функции из $\mathbb{N}$ в $\mathbb{N}$ является арифметическим подмножеством $\mathbb{N}^2$. Однако эта задача далеко не тривиальна — читатель может убедиться в этом, попробовав доказать, например, арифметичность показательной функции с основанием 2, т. е. арифметичность множества

$$\{\langle x, y \rangle \mid y = 2^x\}.$$

В.1. Язык адресных программ. Мы опишем сейчас некоторый класс алгоритмов специального вида, которые будут называться адресными программами. Эти программы будут напоминать «программы в машинных кодах» для реально существующих ЭВМ.

Адресная программа представляет собой последовательность команд, пронумерованных по порядку. Каждая команда имеет один из следующих видов:

1° $R(a) \leftarrow b$ (присвоение значения);
2° $R(a) \leftarrow R(b)$ (пересылка);
3° $R(a) \leftarrow R(b) + R(c)$ (сложение);
4° $R(a) \leftarrow R(b) \cdot R(c)$ (умножение);
5° **ИДТИ К** n (безусловный переход);

6° **ЕСЛИ** $R(a)=R(b)$ **ТО ИДТИ К** m **ИНАЧЕ К** n (условный переход);

7° **СТОП** (останов).

Здесь a, b и c — произвольные натуральные числа («номера регистров»), m, n — натуральные числа, являющиеся порядковыми номерами некоторых команд программы. Последней командой программы должна быть команда вида 7°. В скобках указаны названия видов команд. Вот простой пример адресной программы:

Пример 1.

1 $R(1) \leftarrow 1$

2 $R(2) \leftarrow 1$

3 $R(3) \leftarrow 1$

4 $R(2) \leftarrow R(2) \cdot R(1)$

5 $R(1) \leftarrow R(1) + R(3)$

6 **ЕСЛИ** $R(1)=R(0)$ **ТО ИДТИ К 7 ИНАЧЕ К 4**

7 $R(0) \leftarrow R(2)$

8 **СТОП**

Адресные программы могут выполняться на (воображаемых) адресных машинах.

Адресная машина имеет бесконечное число устройств, предназначенных для хранения (запоминания) натуральных чисел. Эти устройства называются регистрами. В каждом регистре в каждый момент времени хранится (запоминается) ровно одно число. Регистры снабжаются номерами 0, 1, 2, ... и обозначаются соответственно $R(0)$, $R(1)$, $R(2)$ и т. д.

Адресная машина выполняет программу в порядке номеров команд; этот порядок нарушается лишь при выполнении команд условного и безусловного переходов. Прежде чем давать точные определения, опишем работу адресной машины по программе из примера 1. Пусть до начала работы в регистре $R(0)$ находится число 100, в остальных — нули. Первые три команды задают начальные значения регистров $R(1)$—$R(3)$. Содержимое регистра $R(3)$ не меняется во время дальнейшего выполнения программы, содержимое регистра $R(1)$ время от времени увеличивается на 1 (команда 5; напомним, что в $R(3)$ всегда хранится 1), со-

держимое $R(2)$ время от времени умножается на значение, хранящееся в $R(1)$. Выполнение программы заканчивается, когда содержимое $R(1)$ становится равным содержимому $R(0)$. Изменение содержимого регистров с течением времени отражено в следующей таблице:

Номер команды	$R(0)$	$R(1)$	$R(2)$	$R(3)$	$R(4)$
1	100	0	0	0	0
2	100	1	0	0	0
3	100	1	1	0	0
4	100	1	1	1	0
5	100	1	1	1	0
6	100	2	1	1	0
4	100	2	1	1	0
5	100	2	2	1	0
6	100	3	2	1	0
4	100	3	2	1	0
5	100	3	6	1	0
6	100	4	6	1	0
4	100	4	6	1	0
. . .	. . .	. . .	. . .	. . .	. . .
6	100	99	98!	1	0
4	100	99	98!	1	0
5	100	99	99!	1	0
6	100	100	99!	1	0
7	100	100	99!	1	0
8	99!	100	99!	1	0

В результате работы этой программы число 99! $(=1\cdot 2\cdot \ldots \cdot 99)$ помещается в регистр $R(0)$. Если вначале в $R(0)$ хранилось не 100, а 200, то в регистр $R(0)$ будет по окончании работы помещено число 199! $(=1\cdot 2\cdot \ldots \cdot 199)$. Если же до начала работы программы во всех регистрах хранились нули, то выполнение программы никогда не закончится.

Дадим точные определения. *Состоянием* адресной машины называется бесконечная последовательность натуральных чисел $s=(s_0, s_1, \ldots)$, в которой почти все (все, кроме конечного числа) члены равны 0 (такие последовательности называются *финитными*). Если $s_0=0$, состояние называется *заключительным* (состоянием остановки); если $s_0 \geqslant 1$, состояние называется *рабочим*, а s_0 — *номером выполняемой команды*. Число s_{i+1} называется *содержимым i-го регистра*.

Пусть p — некоторая адресная программа, $s = (s_0, s_1, \ldots)$ — рабочее состояние. Будем говорить, что программа p *применима* к состоянию s, если s_0 — номер одной из команд программы p (команды с номером s_0 может не быть, если s_0 слишком велико). В этом случае мы определим некоторое состояние s', называемое *непосредственным результатом применения программы* p к состоянию s. Состояние $s' = (s'_0, s'_1, \ldots)$ определяется следующим образом:

1° если команда с номером s_0 имеет вид $R(a) \leftarrow b$, то $s'_0 = s_0 + 1$, $s'_{i+1} = s_{i+1}$ при $i \neq a$, $s'_{a+1} = b$ (содержимое всех регистров, кроме a-го, не меняется, в a-й регистр помещается число b; машина переходит к выполнению следующей команды);

2° если команда с номером s_0 имеет вид $R(a) \leftarrow R(b)$, то $s'_0 = s_0 + 1$, $s'_{i+1} = s_{i+1}$ при $i \neq a$, $s'_{a+1} = s_{b+1}$ (содержимое всех регистров, кроме a-го, не меняется; в a-й регистр помещается содержимое b-го регистра; машина переходит к выполнению следующей по порядку команды);

3° если команда с номером s_0 имеет вид $R(a) \leftarrow R(b) + R(c)$, то $s'_0 = s_0 + 1$, $s'_{i+1} = s_{i+1}$ при $i \neq a$, $s'_{a+1} = s_{b+1} + s_{c+1}$ (содержимое всех регистров, кроме a-го, не меняется, в a-й регистр помещается сумма содержимого b-го и c-го регистров; машина переходит к выполнению следующей команды);

4° если команда с номером s_0 имеет вид $R(a) \leftarrow R(b) \cdot R(c)$, то $s'_0 = s_0 + 1$, $s'_{i+1} = s_{i+1}$ при $i \neq a$, $s'_{a+1} = s_{b+1} \cdot s_{c+1}$ (этот случай отличается от предыдущего лишь заменой сложения на умножение);

5° если команда имеет вид **ИДТИ К** n, то $s'_0 = n$, $s'_{i+1} = s_{i+1}$ при всех i (содержимое регистров не меняется, машина переходит к выполнению команды номер n);

6° если команда с номером s_0 имеет вид **ЕСЛИ** $R(a) = R(b)$ **ТО ИДТИ К** m **ИНАЧЕ К** n, то $s'_{i+1} = s_{i+1}$ при всех i, $s'_0 = m$, если $s_{a+1} = s_{b+1}$; если же $s_{a+1} \neq s_{b+1}$, то $s'_0 = n$ (содержимое регистров не меняется, машина переходит к выполнению команды номер m, если содержимое a-го регистра равно содержимому b-го регистра, и к выполнению команды номер n в противном случае);

7° если команда имеет вид **СТОП**, то $s'_{i+1} = s_{i+1}$ при всех i и $s'_0 = 0$ (машина переходит в заключительное состояние).

Определение непосредственного результата применения адресной программы к состоянию закончено. Заметим, что если программа p применима к состоянию s, то либо непосредственный результат применения является заключительным состоянием, либо к нему применима программа p (мы предполагаем, что номера команд в операторах перехода в программе p являются номерами команд программы p и что последняя команда — команда останова).

Протоколом применения адресной программы p называется последовательность состояний s^0, s^1, ..., s^k, в которой каждое следующее состояние является непосредственным результатом применения p к предыдущему, а последнее состояние является заключительным. Состояние s^0 называется *начальным* состоянием протокола. Существует не более одного протокола данной адресной программы p с данным начальным состоянием; такого протокола не существует, если p неприменима к s^0 или если в последовательности, возникающей при многократном применении p к s^0, не встречается заключительное состояние.

Пусть p — адресная программа, k — натуральное число. Рассмотрим функцию f из $\mathbb{N}^k$ в $\mathbb{N}$, определяемую так: значение f на наборе $\langle a_1, \ldots, a_k \rangle$ есть b если существует протокол применения адресной программы p, начальным состоянием которого является $(1, a_1, a_2, \ldots, a_k, 0, 0, \ldots)$, а b есть содержимое 0-го регистра в заключительном состоянии этого протокола; другими словами, значение f на $\langle a_1, \ldots, a_k \rangle$ есть содержимое регистра $R(0)$ после выполнения программы, если перед ее выполнением числа $a_1, \ldots, a_k$ были помещены в регистры $R(0), \ldots, R(k-1)$, остальные регистры заполнены нулями и программа начала выполняться с первой команды. Функцию f мы будем называть функцией, *k-вычисляемой* программой p (или просто *вычисляемой* программой p, если значение k ясно из контекста).

Пример 2. Пусть p — адресная программа из примера 1. Функция f_1, 1-вычисляемая этой программой, такова: $f_1(0)$ не определено, $f_1(i) = (i-1)!$ при $i \geqslant 1$. Функция f_2, 2-вычисляемая этой программой,

такова:

$$f_2(i,\ j) = \begin{cases} (i-1)!, & \text{если} \quad i \geqslant 1, \\ \text{не определена}, & \text{если} \quad i = 0. \end{cases}$$

Функции, k-вычисляемые адресными программами, назовем *адресно вычислимыми* функциями k аргументов. Очевидно, что все адресно вычислимые функции вычислимы; с другой стороны, все вычислимые функции, известные в настоящее время, оказываются адресно вычислимыми. Таким образом, есть основания принять гипотезу о совпадении классов вычислимых функций из $\mathbb{N}^k$ в $\mathbb{N}$ и адресно вычислимых функций. Приняв эту гипотезу, мы в следующих пунктах докажем утверждение аксиомы арифметичности.

В.2. Расширенный арифметический язык. Вспомогательным средством при доказательстве арифметичности адресно вычислимых функций будет служить расширенный арифметический язык. Чтобы определить его, следует внести в определение языка арифметики из § 4 некоторые изменения.

В алфавит языка добавим два новых символа v (символ для образования одноместных функциональных переменных) и w (символ для образования двуместных функциональных переменных). Слова вида (v^n) будут называться *одноместными функциональными переменными*, а слова вида (w^n) — *двуместными функциональными переменными.* (Здесь $n \geqslant 1$.) Сокращенными обозначениями для одноместных и двуместных функциональных переменных будут служить v_n и w_n. Подразумеваемыми значениями одноместных и двуместных функциональных переменных будут всюду определенные функции от одного и соответственно двух натуральных аргументов с натуральными значениями. Переменные x_n мы будем называть *числовыми* переменными.

Понятие *терма* расширенного арифметического языка определим так:

1° числовая переменная есть терм;

2° если t и u — термы, то $(t+u)$ и $(t \cdot u)$ — термы;

3° если p — одноместная функциональная переменная, а t — терм, то $p(t)$ — терм;

4° если r — двуместная функциональная переменная, а t и u — термы, то $r(t,\ u)$ — терм.

Пример 1. Слова $(v_4(x_1)+x_2)$, $v_4(v_5(w_2(x_1, x_2)))$, $w_2(w_2(x_1, x_4), x_7)$ являются термами расширенного арифметического языка.

Как и раньше, *элементарной формулой* называется равенство двух термов; разумеется, имеются в виду термы расширенного арифметического языка. *Формулы* расширенного арифметического языка определяются, как в § 4, при этом в 4° переменная ξ может быть числовой, одноместной функциональной или двуместной функциональной переменной.

Пример 2. Слова $\forall v_1(v_1(x_1)=v_1(x_2))$, $\forall x_1 \forall x_2(v_1(x_1)=v_1(x_2))$, $\forall w_1 \forall x_1 \forall x_2(w_1(x_1, x_1)= = w_1(x_2, x_1))$ являются формулами.

Параметры термов и формул определяются, как в § 4; в качестве параметров могут выступать как числовые, так и функциональные переменные.

Пример 3. Параметрами термов из примера 1 являются v_4, x_1 и x_2 (первый терм), v_4, v_5, w_2, x_1 и x_2 (второй терм), w_2, x_1, x_4 и x_7 (третий терм). Параметрами формул из примера 2 являются x_1 и x_2 (первая формула), v_1 (вторая формула); третья формула не имеет параметров.

Формулы, не имеющие параметров, называются *суждениями* расширенного арифметического языка.

Теперь мы должны определить, какие суждения расширенного арифметического языка мы объявляем истинными. У нас будет два варианта определения истинности для формул расширенного арифметического языка — две *интерпретации* этого языка. В одной из них функциональные переменные будут принимать в качестве значений все (всюду определенные) функции от одного и от двух натуральных аргументов, в другой их значениями будут лишь финитные функции, т. е. функции, отличные от 0 лишь на конечном множестве аргументов. Чтобы не повторять определение дважды, мы будем говорить о классе *допустимых* функций, подразумевая под ним либо класс всех функций, либо класс всех финитных функций.

Определение истинности будет аналогично определению из § 4. Новым для нас будет случай формул, начинающихся с кванторов по функциональным переменным. Здесь мы сталкиваемся со следующей проблемой: хотелось бы назвать, например, формулу вида $\forall v\alpha$ истинной, если для всех допустимых

значений v формула, получающаяся из α подстановкой этих значений вместо v, является истинной. Но в нашем языке нет ничего, что можно было бы подставлять вместо функциональных переменных. Выход из этого положения таков: мы должны ввести в язык, помимо функциональных переменных, и функциональные константы — по одной для каждой допустимой функции.

Дадим точные определения. Выберем некоторый набор символов, находящийся во взаимно однозначном соответствии с множеством допустимых функций. Символы этого набора назовем *функциональными константами*, изображающими соответствующие им функции. Функциональные константы делятся на *одноместные* и *двуместные* в зависимости от числа аргументов у соответствующей функции. Мы будем подставлять функциональные константы вместо функциональных переменных с тем же числом аргументов. Результат подстановки произвольных функциональных констант вместо всех функциональных параметров и произвольных цифр вместо всех числовых параметров некоторого терма (формулы) расширенного арифметического языка назовем *оцененным термом* (*оцененной формулой*). Подстановка производится таким же образом, как в § 4, — заменяются не все вхождения переменных, а лишь не попадающие в зону действия одноименного квантора. Частным случаем оцененного терма является постоянный терм, т. е. терм, не имеющий параметров (и, следовательно, являющийся термом языка арифметики). Частным случаем оцененной формулы является суждение расширенного арифметического языка.

Теперь мы можем дать определения *значений* оцененных термов и формул, вполне аналогичные определениям значений постоянных термов и замкнутых формул (суждений) языка арифметики. Значения оцененных термов определяются так:

1° значением цифры $(|^n)$ является число n;

2° значением оцененного терма $(t + u)$ служит сумма значений оцененных термов t и u, а значением оцененного терма $(t \cdot u)$ служит произведение значений оцененных термов t и u;

3° значением оцененного терма вида $\gamma(t)$, где γ — одноместная функциональная константа, а t — оценен-

ный терм, служит значение функции, изображаемой константой γ, на числе, равном значению оцененного терма t;

4° значением оцененного терма вида $\delta(t, u)$, где δ — двуместная функциональная константа, а t и u — оцененные термы, служит значение функции из $\mathbb{N}^2$ в $\mathbb{N}$, изображаемой константой δ, на паре $\langle$значение t, значение $u\rangle$.

Теперь для определения значений оцененных формул мы можем воспользоваться данным в § 4 определением значений суждений языка арифметики, заменив слово «суждение» на «оцененная формула», «постоянный терм» на «оцененный терм», оговорив в 7° и 8°, что ξ является числовой переменной, и добавив два следующих пункта:

9° оцененная формула $\exists\xi\alpha$, где ξ — функциональная переменная, истинна, если существует такая функциональная константа γ с тем же числом аргументов, что у ξ, что оцененная формула $S^{\xi}_{\gamma}\alpha$ истинна; если такой константы нет, то оцененная формула $\exists\xi\alpha$ ложна;

10° оцененная формула $\forall\xi\alpha$, где ξ — функциональная переменная, истинна, если для всякой функциональной константы γ с тем же числом аргументов, что у ξ, оцененная формула $S^{\xi}_{\gamma}\alpha$ истинна; в противном случае оцененная формула $\forall\xi\alpha$ ложна.

Дав определения значений оцененных формул, мы, в частности, определили значения суждений расширенного арифметического языка. Этот частный случай будет для нас в дальнейшем особенно важен.

Пример 4. Суждение

$$\forall x_1 \forall x_2 (\forall v_1 (v_1(x_1) = v_1(x_2)) \to (x_1 = x_2)),$$

которое можно прочесть так: «если значения всех допустимых функций на x_1 и x_2 совпадают, то $x_1 = x_2$» истинно при любом из двух пониманий допустимости — считаем ли мы допустимыми все функции или только финитные функции.

Пример 5. Суждение

$$\forall v_1 \exists x_1 \forall x_2 (v((x_1 + x_2)) = 0),$$

которое можно прочесть так: «всякая допустимая функция равна 0 для всех достаточно больших значений аргумента», истинно, если допустимыми

считать финитные функции, и ложно, если считать все функции допустимыми.

Пример 6. Суждение

$$\forall w_1 \exists v_1 \forall x_1 (v_1(x_1) = w_1(x_1, x_1))$$

истинно при любом из двух пониманий допустимости.

Пример 7. Следующее суждение утверждает, что существует допустимое взаимно однозначное соответствие между $\mathbb{N}^2$ и $\mathbb{N}$:

$$\exists w_1 (\forall x_1 \exists x_2 \exists x_3 (w_1(x_2, x_3) = x_1) \wedge \wedge \forall x_2 \forall x_3 \forall x_4 \forall x_5 ((w_1(x_2, x_3) = = w_1(x_4, x_5)) \rightarrow ((x_2 = x_4) \wedge (x_3 = x_5)))).$$

Оно истинно, если считать допустимыми все функции, и ложно, если считать допустимыми лишь финитные функции.

Пример 8. Утверждение «при всех x_1 верно неравенство $2^{x_1} \geqslant x_1$» может быть переведено следующей формулой расширенного языка арифметики (при любом из двух пониманий допустимости):

$$\forall x_1 \forall v_1 (((v_1(0) = 1) \wedge \forall x_2 ([x_2 \leqslant x_1] \rightarrow \rightarrow (v_1((x_2 + 1)) = (2 \cdot v_1(x_2))))) \rightarrow [x_1 \leqslant v_1(x_1)]).$$

Здесь $[x_2 \leqslant x_1]$ обозначает $\exists x_3((x_2 + x_3) = x_1)$, а $[x_1 \leqslant v_1(x_1)]$ обозначает $\exists x_3((x_1 + x_3) = v_1(x_1))$. Суждение может быть прочитано так: если v_1 — последовательность натуральных чисел, первый член которой равен 1 и каждый следующий, вплоть до $x_1 + 1$-го, вдвое больше предыдущего, то $v_1(x_1) \geqslant x_1$. Оговорка «вплоть до $x_1 + 1$-го» необходима, если допустимыми являются лишь финитные функции.

Подобно тому как в приложении Б мы интерпретировали формулы языка арифметики с параметрами как выражающие свойства натуральных чисел, мы можем рассматривать формулы расширенного языка как выражающие свойства чисел и функций.

Пример 9. Формула

$$\exists x_3 ((v_1(x_2) + x_3) = v_1(x_1))$$

выражает следующее свойство: значение допустимой функции v_1 на числе x_1 не меньше ее значения на числе x_2. Последнее предложение является (не впол-

не корректным, так как v_1 — функциональная переменная, а не функция, а x_1, x_2 — числовые переменные, но не числа) сокращением для следующего утверждения: результат подстановки вместо x_1 и x_2 некоторых цифр n_1 и n_2 и вместо v_1 некоторой функциональной константы, изображающей допустимую функцию, тогда и только тогда является истинной оценённой формулой расширенного языка арифметики (при любом из двух пониманий допустимости), когда значение этой допустимой функции на числе n_1 не меньше ее значения на числе n_2.

Пример 10. Формула

$$\forall x_1 \forall x_2 \exists x_3 ((v_1(x_1) + x_3) = v_1((x_1 + x_2)))$$

выражает свойство «допустимая функция v_1 является неубывающей».

Даже если ограничиться формулами расширенного языка, не имеющими функциональных параметров, мы все равно приобретаем новые возможности по сравнению с языком арифметики.

Пример 11. Формула

$$\exists v_1 (((v_1(0) = 1) \wedge \forall x_3 ([x_3 \leqslant x_1] \rightarrow$$
$$\rightarrow (v_1((x_3 + 1)) = (2 \cdot v_1(x_3))))) \wedge (v_1(x_1) = x_2)),$$

где $[x_3 \leqslant x_1]$ является (уже привычным для нас) сокращением для $\exists x_2((x_3 + x_2) = x_1)$, выражает упоминавшееся вначале приложения В свойство: «$x_2 = 2^{x_1}$». (Это справедливо при любом из двух пониманий допустимости; если считать допустимыми все функции, то оговорка $[x_3 \leqslant x_1]$ является излишней.)

Свойства натуральных чисел, выражаемые формулами расширенного арифметического языка, назовем *аналитическими* или *слабо аналитическими* в зависимости от того, считаем ли мы допустимыми все функции или только финитные. Отождествляя свойства с множествами удовлетворяющих им объектов, мы будем говорить также об аналитических и слабо аналитических множествах.

Более точно, пусть α — формула расширенного арифметического языка, не содержащая функциональных параметров, а также числовых параметров, отличных от $x_1, \ldots, x_k$. Пусть $n_1, \ldots, n_k$ — набор цифр. Подставив их вместо переменных $x_1 \ldots x_k$, мы

получим суждение расширенного арифметического языка. Множество тех $\langle n_1, \ldots, n_k \rangle$, при которых это суждение истинно, будем называть *сопряженным* с формулой α (если допустимыми считать все функции) или *слабо сопряженным* с ней (если допустимыми считать лишь финитные функции). Множества, сопряженные (слабо сопряженные) с некоторыми формулами расширенного арифметического языка, будем называть *аналитическими* (соответственно *слабо аналитическими*).

Пример 12. Как показывает пример 11, множество $\{\langle x_1, x_2 \rangle \mid x_2 = 2^{x_1}\}$ является аналитическим, а также слабо аналитическим.

Всякое арифметическое множество, очевидно, является и аналитическим, и слабо аналитическим. Впоследствии мы докажем, что все слабо аналитические множества арифметичны; это обстоятельство оправдывает выбор длинного выражения «слабо аналитические» в качестве временного термина для их обозначения. Но не всякое аналитическое множество арифметично. Можно доказать, что множество номеров истинных суждений языка арифметики при любой вычислимой нумерации слов алфавита А аналитично, в то время как, согласно теореме Тарского (см. приложение Б), оно не арифметично. (Заметим в скобках, что рассуждение, аналогичное доказательству теоремы Тарского, позволяет установить, что множество суждений расширенного языка арифметики, истинных, если допустимыми считать все функции, аналитичным не является.) В следующем пункте мы покажем, что график всякой адресно вычислимой функции является слабо аналитическим множеством; в сочетании с упоминавшимся результатом об арифметичности всех слабо аналитических множеств это даст нам утверждение об арифметичности всех адресно вычислимых функций.

В.3. Выразимость адресно вычислимых функций в расширенном арифметическом языке. В этом пункте мы докажем, что график всякой адресно вычислимой функции является слабо аналитическим множеством. Мы докажем впоследствии (В.4—В.6), что всякое слабо аналитическое множество арифметично, и это завершит доказательство арифметичности адресно вы-

числимых функций и, следовательно, арифметичности множеств, перечисляемых такими функциями.

Пусть p — некоторая адресная программа. Докажем, что некоторые свойства, связанные с программой p, выразимы в расширенном языке арифметики. Говоря в дальнейшем об истинности оцененных формул расширенного арифметического языка, мы будем считать допустимыми лишь финитные функции, не оговаривая этого особо.

Напомним, что состояния адресных машин представляют собой последовательности натуральных чисел, в которых все члены, начиная с некоторого, равны 0; такие последовательности суть не что иное, как финитные функции.

Лемма B.1. *Свойство «состояние v_2 является непосредственным результатом применения программы p к состоянию v_1» выразимо в расширенном языке арифметики. (Это означает, что существует такая формула α расширенного арифметического языка, параметрами которой являются одноместные функциональные переменные v_1 и v_2, что результат подстановки вместо v_1 и v_2 двух констант для финитных функций тогда и только тогда является истинной оцененной формулой, когда непосредственным результатом применения программы p к состоянию, изображаемому первой константой, является состояние, изображаемое второй константой.)*

Доказательство. Пусть задана программа p, опишем способ построения требуемой формулы. (Эта формула будет, конечно, зависеть от выбора p.) Нужная нам формула α будет иметь вид $\alpha_1 \wedge \ldots \wedge \alpha_n$ (опущенные скобки можно поставить любым образом). Число n будет равно числу команд программы, и формула α_i будет соответствовать i-й команде. Каждая из формул α_i может быть одного из семи типов, в соответствии с семью типами команд, возможных для адресных машин. Эти формулы строятся в соответствии с семью пунктами определения непосредственного результата применения; способ их построения поясним на примерах.

Пример 1. Пусть 37-я команда программы имеет вид

$$37 \quad R(16) \leftarrow R(2) \cdot R(16).$$

В этом случае формула α_{37} будет такой:

$$(v_1(0)=37)\to(\forall x_1(\neg(x_1=16)\to(v_2((x_1+1))= \\ =v_1((x_1+1))))\wedge(v_2(17)=(v_1(17)\cdot v_1(3)))).$$

Пример 2. Пусть 81-я команда программы имеет вид

81 **ЕСЛИ** $R(3)=R(4)$ **ТО ИДТИ К** 7 **ИНАЧЕ К** 23.

В этом случае формула α_{81} будет такой:

$$(v_1(0)=81)\to(\forall x_1(v_2(x_1+1)=v_1(x_1+1))\wedge(((v_1(4)= \\ =v_1(5))\to(v_2(0)=7))\wedge(\neg(v_1(4)=v_1(5))\to(v_2(0)=23)))).$$

Доказательство леммы закончено.

Следующим шагом будет построение формулы, выражающей свойство «быть протоколом применения адресной программы p длины x_1+1». Протокол является последовательностью состояний, т. е. последовательностью финитных функций.

В нашем языке нет последовательностей функций, но есть объекты, их заменяющие: мы отождествим последовательность функций s^0, s^1, ... от одного натурального аргумента с функцией $S(n,m)=s^n(m)$ от двух натуральных аргументов. В соответствии с этим отождествлением мы будем называть всюду определенную функцию S из $\mathbb{N}^2$ в $\mathbb{N}$ *изображением протокола* программы p длины $k+1$, если последовательность s^0, ..., s^k функций от одного аргумента, определяемых по формуле $s^i(x)=S(i,x)$, является протоколом применения адресной программы p.

Лемма В.2. *Существует формула* β *с двуместным функциональным параметром* w_1, *двумя одноместными параметрами* v_1, v_2 *и с одним числовым параметром* x_1, *выражающая следующее свойство*:

«w_1 *является изображением протокола длины* x_1+1,
v_1 *является начальным состоянием этого протокола,*
v_2 *является заключительным состоянием этого протокола*».

Доказательство. Искомая формула имеет следующий вид:

$$(([v_1=w_1^0]\wedge[v_2=w_1^{x_1}])\wedge(v_2(0)=0))\wedge \\ \wedge\forall x_2\forall v_3\forall v_4(([x_2+1\leqslant x_1]\wedge \\ \wedge([v_3=w_1^{x_2}]\wedge[v_4=w_1^{x_2+1}]))\to$$

$\to$ [v_1 является непосредственным результатом применения программы p к v_3]).

В этой записи $[v_1 = w_1^0]$ есть сокращение для $\forall x_3 (v_1(x_3) = w_1(0, x_3))$; сокращения $[v_2 = w_1^{x_1}]$, $[v_3 = w_1^{x_2}]$ и $[v_4 = w_1^{x_2+1}]$ расшифровываются аналогично — последнее, например, обозначает формулу

$$\forall x_3 (v_4(x_3) = w_1((x_2 + 1), x_3));$$

[v_4 является непосредственным результатом применения программы p к v_3] обозначает формулу из леммы В.1, в которой переменные v_1 и v_2 заменены соответственно на v_3 и v_4.

Теперь все готово для доказательства слабой аналитичности графиков адресно вычислимых функций.

Теорема В.1. *График адресно вычислимой функции из $\mathbb{N}^k$ в $\mathbb{N}$ является слабо аналитическим множеством.*

Доказательство. Пусть f — адресно вычислимая функция из $\mathbb{N}^k$ в $\mathbb{N}$, p — адресная программа, ее вычисляющая. График функции f состоит из таких наборов $\langle x_1, \ldots, x_k, x_{k+1}\rangle$, для которых существует протокол w_1 некоторой длины с начальным состоянием v_1 и заключительным состоянием v_2, для которого

$$v_1(0) = 1,\ v_1(1) = x_1,\ \ldots,\ v_1(k) = x_k,$$
$$v_1(x) = 0 \text{ при } x \geqslant k + 1,\ v_2(1) = x_{k+1}.$$

Записывая предыдущую фразу в виде формулы расширенного арифметического языка, получаем искомую формулу — формулу, с которой слабо сопряжен график функции f. Теорема доказана.

В следующих пунктах В.4—В.6 мы докажем, что всякое слабо аналитическое множество и, следовательно, график всякой адресно вычислимой функции являются арифметическими множествами.

В.4. Сведение расширенного арифметического языка к обычному. В этом пункте мы будем доказывать, что всякое слабо аналитическое множество арифметично, т. е. что добавление к языку арифметики переменных, пробегающих множества всех *финитных* функций одного и двух натуральных аргументов, не увеличивает выразительных возможностей языка.

(Как уже отмечалось, условие финитности существенно: добавляя переменные, пробегающие множество *всех* функций, мы получаем существенно более выразительный язык.) Попытаемся в самых общих чертах объяснить, почему добавление переменных для обозначения финитных функций несущественно. Дело в том, что множество этих функций счетно, их можно закодировать натуральными числами (и это кодирование окажется арифметическим в уточняемом ниже смысле), и мы можем говорить о кодах функций вместо того, чтобы говорить о самих функциях. Тем самым мы ограничиваемся рассмотрением натуральных чисел.

Уточним сказанное. Пусть ν — отображение, сопоставляющее каждому элементу множества $\mathbb{N}^k$, т. е. каждому набору (кортежу) из k натуральных чисел, некоторую (всюду определенную) финитную функцию одного аргумента. Назовем его *способом кодирования* (или, короче, просто *кодированием*) *финитных функций одного аргумента с помощью элементов* $\mathbb{N}^k$, если каждая финитная функция соответствует по крайней мере одному (но, возможно, и не только одному) элементу $\mathbb{N}^k$; если набору $\langle a_1, \ldots, a_k\rangle$ соответствует функция s, то будем называть этот набор *кодом* функции s (при данном способе кодирования). Кодирование назовем *арифметическим*, если множество

$$\{\langle a_1, \ldots, a_k, x, y\rangle \mid \text{значение финитной функции с кодом } \langle a_1, \ldots, a_k\rangle \text{ на числе } x \text{ равно } y\}$$

является арифметическим.

Ключевым пунктом нашего доказательства арифметичности слабо аналитических множеств является следующее утверждение:

(*) *при некотором k существует арифметический способ кодирования финитных функций элементами* $\mathbb{N}^k$.

В пп. В.5 и В.6 будут предложены два различных доказательства этого утверждения. А сейчас мы покажем, как из него вытекает арифметичность слабо аналитических множеств.

Аналогично данному выше определению арифметического кодирования финитных функций одного аргумента можно дать определение арифметического

кодирования (всюду определенных) финитных функций двух аргументов. Оказывается, что существование такового вытекает из существования арифметического кодирования для финитных функций одного аргумента — желая закодировать функцию f из $\mathbb{N}^2$ в $\mathbb{N}$, мы сначала кодируем ее «сечения», т. е. функции $f_n(x) = f(n, x)$, а затем кодируем последовательность кодов сечений. Более точно, имеет место следующая простая

Лемма В.3. *Если ν — арифметическое кодирование финитных функций одного аргумента элементами $\mathbb{N}^k$, причем $\langle 0, 0, \ldots, 0\rangle$ есть код нулевой финитной функции, то функция μ, сопоставляющая набору $\langle a_1^1, \ldots, a_k^1, \ldots, a_1^k, \ldots, a_k^k\rangle$ функцию из $\mathbb{N}^2$ в $\mathbb{N}$, равную*

$$\nu\left(\nu\left(a_1^1, \ldots, a_k^1\right)(p), \ldots, \nu\left(a_1^k, \ldots, a_k^k\right)(p)\right)(q)$$

на паре $\langle p, q\rangle$, является арифметическим кодированием финитных функций двух аргументов элементами $\mathbb{N}^{k^2}$.

Легко видеть, что ограничение «$\langle 0, 0, \ldots, 0\rangle$ есть код нулевой последовательности» несущественно: мы можем переделать любое арифметическое кодирование в кодирование с таким свойством, обменяв друг с другом два кодовых обозначения; при этом арифметичность сохранится.

Итак, мы предполагаем, что зафиксировано некоторое арифметическое кодирование ν финитных функций одного аргумента элементами $\mathbb{N}^k$, а также некоторое арифметическое кодирование μ финитных функций двух аргументов элементами $\mathbb{N}^l$.

Мы построим для каждой формулы расширенного арифметического языка ее «перевод» — формулу языка арифметики, утверждающую то же самое, что исходная формула, но не о функциях, а об их кодах. Для удобства мы добавим в язык арифметики новые переменные для чисел — по k новых переменных $V_i^1, \ldots, V_i^k$ для каждой одноместной функциональной переменной v_i и по l новых переменных $W_i^1, \ldots, W_i^l$ для каждой двуместной функциональной переменной w_i. Ясно, что класс арифметических множеств не изменится от такого расширения — не все ли равно, как

называются переменные! Дадим теперь точное определение перевода.

Пусть α — формула расширенного арифметического языка, имеющая числовые параметры $x_{p_1}, \ldots, x_{p_m}$, одноместные функциональные параметры $v_{q_1}, \ldots, v_{q_n}$ и двуместные функциональные параметры $w_{r_1}, \ldots, w_{r_s}$. Пусть β — формула арифметического языка, параметры которой содержатся среди $x_{p_1}, \ldots, x_{p_m}, V^l_{q_1}, \ldots, V^k_{q_1}, \ldots$ $\ldots, V^1_{q_n}, \ldots, V^k_{q_n}, W^1_{r_1}, \ldots, W^l_{r_1}, \ldots, W^1_{r_s}, \ldots, W^l_{r_s}$. Формула β называется *переводом* формулы α, если для любых натуральных чисел $\boldsymbol{x}_{p_1}, \ldots, \boldsymbol{x}_{p_m}, \boldsymbol{V}^1_{q_1}, \ldots$ $\ldots, \boldsymbol{V}^k_{q_n}, \boldsymbol{W}^1_{r_1}, \ldots, \boldsymbol{W}^l_{r_s}$ результат подстановки соответствующих им цифр вместо $x_{p_1}, \ldots, x_{p_m}, V^1_{q_1}, \ldots$ $\ldots, V^k_{q_n}, W^1_{r_1}, \ldots, W^l_{r_s}$ в β является истинным суждением языка арифметики тогда и только тогда, когда результат подстановки $\boldsymbol{x}_{p_1}, \ldots, \boldsymbol{x}_{p_m}, \nu\left(\boldsymbol{V}^1_{q_1}, \ldots, \boldsymbol{V}^k_{q_1}\right)\ldots$ $\ldots, \nu\left(\boldsymbol{V}^1_{q_n}, \ldots, \boldsymbol{V}^k_{q_n}\right), \mu\left(\boldsymbol{W}^1_{r_1}, \ldots, \boldsymbol{W}^l_{r_1}\right), \ldots, \mu\left(\boldsymbol{W}^1_{r_s}, \ldots\right.$ $\left.\ldots, \boldsymbol{W}^l_{r_s}\right)$ (точнее, не самих чисел и функций, а изображающих их констант) вместо $x_{p_1}, \ldots, x_{p_m}, v_{q_1}, \ldots$ $\ldots, v_{q_n}, w_{r_1}, \ldots, w_{r_s}$ в α является истинной оцененной формулой.

Теорема В.2. *Всякая формула расширенного языка арифметики имеет перевод.*

Прежде чем доказывать эту теорему, отметим, что из ее частного случая (случая формул без функциональных параметров), очевидно, следует интересующее нас утверждение об арифметичности слабо аналитических множеств: если множество слабо сопряжено с формулой расширенного языка арифметики, то оно сопряжено с ее переводом.

Доказательство. Предположим, что для элементарных формул расширенного языка переводы построены. Покажем, как построить их для остальных формул.

Лемма В.4. 1° *Если β — перевод α, то $\neg\beta$ — перевод $\neg\alpha$;*

2° *если β_1 и β_2 — переводы α_1 и α_2, то*

$$(\beta_1 \wedge \beta_2),\ (\beta_1 \vee \beta_2),\ (\beta_1 \rightarrow \beta_2),\ (\beta_1 \leftrightarrow \beta_2)$$

являются переводами формул

$$(\alpha_1 \wedge \alpha_2),\ (\alpha_1 \vee \alpha_2),\ (\alpha_1 \to \alpha_2),\ (\alpha_1 \leftrightarrow \alpha_2);$$

3° *если* β — *перевод* α, Q — *любой из знаков* $\forall$, $\exists$, *то*

$$Qx_i\beta \text{ — перевод } Qx_i\alpha,$$

$$QV_i^1 \dots QV_i^k\beta \text{ — перевод } Qv_i\alpha,$$

$$QW_i^1 \dots QW_i^l\beta \text{ — перевод } Qw_i\alpha.$$

Эта лемма непосредственно вытекает из определения перевода и определения истинности формул. Применяя ее, мы видим, что достаточно построить переводы элементарных формул, т. е. формул вида $(t=u)$. Заменяя их на $\exists\xi((t=\xi) \wedge (u=\xi))$ (ξ — числовая переменная, не входящая ни в t, ни в u) и применяя утверждения 2° и 3° доказанной леммы, мы видим, что достаточно перевести формулы вида $(t=\xi)$, где t — терм расширенного языка, а ξ — числовая переменная. Возможность перевода таких формул докажем индукцией по построению терма t:

1° если t — переменная или цифра, то в качестве перевода можно взять саму формулу;

2° если t есть (u_1+u_2), то, заменив формулу

$$((u_1+u_2)=\xi) \text{ на } \exists\eta_1\exists\eta_2(((u_1=\eta_1) \wedge \\ \wedge (u_2=\eta_2)) \wedge (\xi=(\eta_1+\eta_2))),$$

где η_1 и η_2 — числовые переменные, не входящие в t и отличные от ξ, мы сможем сослаться на предположение индукции и лемму В.4;

3° случай, в котором t есть $(u_1 \cdot u_2)$, аналогичен предыдущему;

4° если t есть $p(u)$, где u — терм, а p — одноместная функциональная переменная, то, заменяя формулу $(p(u)=\xi)$ на $\exists\eta((u=\eta) \wedge (p(\eta)=\xi))$ (где η — переменная, не входящая в u и отличная от ξ), мы видим, что достаточно перевести формулу $(p(\eta)=\xi)$; это возможно в силу предположенной арифметичности кодирования;

5° случай, в котором $t=r(u_1, u_2)$, где u_1, u_2 — термы, r — двуместная функциональная переменная, аналогичен предыдущему.

Пример 1. В качестве перевода формулы

$$\forall x_1(v_1(x_1)=v_2(x_1))$$

можно взять формулу

$\forall x_1 \exists x_2$ ([значение одноместной функции с кодом

$\langle V_1^1, \ldots, V_1^k \rangle$ в x_1 есть x_2] $\wedge$

$\wedge$ [значение одноместной функции с кодом

$\langle V_2^1, \ldots, V_2^k \rangle$ в x_1 есть x_2]),

где записи в квадратных скобках обозначают формулы языка арифметики, выражающие записанные внутри скобок свойства и существующие в силу арифметичности кодирования.

Итак, для завершения доказательства арифметичности слабо аналитических множеств осталось лишь построить арифметическое кодирование финитных функций одного аргумента.

В.5. Первый способ построения арифметического кодирования — способ Гёделя. Мы начнем построение арифметического кодирования со следующего замечания: достаточно доказать, что существует всюду определенная арифметическая функция $\beta(x_1, \ldots, x_l, y)$ со следующим свойством:

(*) *для всякой конечной последовательности* $n_0, \ldots, n_k$ *натуральных чисел существуют такие* $a_1, \ldots, a_l$, *что* $\beta(a_1, \ldots, a_l, 0) = n_0$, $\beta(a_1, \ldots, a_l, 1) = n_1, \ldots, \beta(a_1, \ldots, a_l, k) = n_k$. (При этом значения $\beta(a_1, \ldots, a_l, y)$ при $y > k$ могут быть любыми.) В самом деле, пусть β обладает этим свойством. Тогда функция ν, сопоставляющая набору $\langle x_1, \ldots, x_l, l \rangle$ финитную функцию $s(y)$, равную $\beta(x_1, \ldots, x_l, y)$ при $y \leqslant l$ и равную 0 при $y > l$, является искомым арифметическим кодированием финитных функций одного аргумента элементами $\mathbb{N}^{l+1}$. То, что это кодирование, вытекает из свойства (*); то, что оно арифметично, вытекает из арифметичности функции β и арифметичности свойства $y \leqslant l$.

Итак, нам достаточно построить при некотором натуральном l функцию от $l+1$ аргумента, обладающую свойством (*). В качестве такой функции мы, следуя Гёделю, возьмем функцию

$$\beta(x_1, x_2, y) = (\text{остаток от деления } x_1 \text{ на } x_2(y+1)+1).$$

Арифметичность этой функции следует из арифметичности свойства «x_3 есть остаток от деления x_1 на x_2»,

выражаемого формулой $[x_3 < x_2] \wedge \exists x_4 (x_1 = = ((x_2 \cdot x_4) + x_3))$, где $[x_3 < x_2]$ обозначает формулу $\exists x_5 (((x_3 + x_5) + 1) = x_2)$. Чтобы доказать свойство (*), нам придется рассмотреть некоторые простые факты из теории чисел; их доказательства можно прочесть, например, в книге Оре О. Приглашение в теорию чисел. – М.: Наука, 1980. Всюду дальше в этом пункте, говоря о числах, мы имеем в виду натуральные числа.

Число a называется делителем числа b, если $a = bc$ при некотором c. Если a является делителем чисел b и c, то оно является делителем их суммы и разности. Число $p > 1$, не имеющее делителей, отличных от 1 и p, называется простым. Всякое число разлагается на простые множители, причем однозначно: его разложения могут отличаться лишь порядком сомножителей. Если произведение нескольких чисел делится на простое число p, то один из сомножителей делится на p. Числа a и b называются взаимно простыми, если у них нет общих делителей, отличных от 1. Числа a и b взаимно просты тогда и только тогда, когда в их разложениях на простые множители нет общих множителей. Если числа $a_1, \ldots, a_n$ попарно взаимно просты, а число b делится на любое из них, то b делится на $a_1 \cdot a_2 \cdot \ldots \cdot a_n$.

Пусть $a_0, \ldots, a_k$ — попарно взаимно простые числа. Рассмотрим, какие наборы остатков $\langle r_0, \ldots, r_k \rangle$ возможны при делении некоторого числа x на числа $a_0, \ldots, a_k$. Остаток при делении на a_i — одно из чисел $0, 1, \ldots, a_i - 1$; таким образом, существует $a_0 \cdot a_1 \cdot \ldots \cdot a_k$ возможных наборов остатков. Следующая лемма утверждает, что все возможности действительно реализуются.

Лемма В.5. (Китайская теорема об остатках.) *Пусть $a_0, \ldots, a_k$ — попарно взаимно простые числа, $r_0, \ldots, r_k$ — некоторые числа, причем $r_i < a_i$ при всех i. Тогда существует число x, дающее при делении на любое из чисел a_i остаток r_i.*

Доказательство. Назовем два числа эквивалентными, если они дают одинаковые остатки при делении на любое из a_i. Если два числа эквивалентны, то их разность делится на любое из чисел a_i и, следовательно, на $a_0 \cdot \ldots \cdot a_k$ (в силу взаимной простоты). Поэтому никакие два из чисел $0, 1, \ldots$

$\ldots, a_0 \cdot \ldots \cdot a_k - 1$ не эквивалентны и каждому соответствует свой набор остатков. Но этих чисел столько же, сколько возможных наборов. Поэтому любой набор $\langle r_0, \ldots, r_k \rangle$, у которого $r_i < a_i$ при всех i, является набором остатков от деления некоторого числа x на $a_0, \ldots, a_k$.

Лемма В.6. *Для всякого числа n можно указать такое b, что числа $b+1, 2b+1, \ldots, nb+1$ попарно взаимно просты. Число b можно выбрать бо́льшим любого заданного наперед натурального числа.*

Доказательство. Заметим сначала, что если p — общий простой делитель чисел $kb+1$ и $lb+1$, то p является делителем их разности — числа $(k-l)b$. Но делить число b он не может, так как иначе числа $kb+1$ и $lb+1$ давали бы остаток 1 при делении на p. Поэтому $k-l$ делится на p. Из сказанного следует, что числа $b+1, \ldots, nb+1$ будут взаимно просты, если они не будут иметь общих делителей, меньших n. Этого можно достигнуть, взяв, например, b кратным $1 \cdot 2 \cdot \ldots \cdot n$; тогда числа $b+1, \ldots, nb+1$ будут давать остаток 1 при делении на любое число от 2 до n.

Теперь мы легко можем доказать свойство (*) для построенной нами функции β. В самом деле, пусть $n_0, \ldots, n_k$ — любые натуральные числа; нам надо найти такие x_1 и x_2, чтобы остаток от деления x_1 на $x_2(i+1)+1$ был равен n_i при $i \leqslant k$. Согласно лемме В.6 можно найти такое x_2, что числа $x_2+1, \ldots, x_2(k+1)+1$ попарно взаимно просты и x_2 больше любого из чисел $n_0, \ldots, n_k$; осталось выбрать x_1 с помощью леммы В.5.

Построение арифметического кодирования методом Гёделя закончено. В следующем пункте мы рассмотрим другой метод построения арифметического кодирования, не использующий теоретико-числовых соображений и предложенный Смальяном в книге Smullyan R. M. Theory of formal systems. — Princeton, 1961, русский перевод которой (Смальян Р. Теория формальных систем) вышел в издательстве «Наука» в 1981 г.

В.6. Второй способ построения арифметического кодирования — способ Смальяна. Введем понятие арифметического кодирования конечных подмножеств $\mathbb{N}$ натуральными числами, аналогичное понятию ко-

дирования финитных функций элементами $\mathbb{N}^1$. А именно, функцию τ, сопоставляющую всем натуральным числам некоторые подмножества $\mathbb{N}$, назовем *кодированием*, если любое конечное подмножество $\mathbb{N}$ является значением τ на некотором числе; если $\tau(y) = A$, то будем называть число y *кодом* множества A (относительно τ). Кодирование назовем *арифметическим*, если множество

$$\{\langle x, y\rangle \mid x \in \tau(y)\}$$

является арифметическим подмножеством $\mathbb{N}^2$.

Заметим, что (в нарушение аналогии с определением кодирования финитных функций) мы не требуем, чтобы подмножества, соответствующие всем натуральным числам, были конечными.

Арифметические кодирования конечных подмножеств $\mathbb{N}$ натуральными числами существуют. Прежде чем доказывать это, мы покажем, как отсюда вытекает существование арифметического кодирования финитных функций одного аргумента. Итак, пусть τ — арифметическое кодирование конечных подмножеств натуральными числами.

Лемма В.7. *Существует арифметическая функция из $\mathbb{N}^2$ в $\mathbb{N}$, определенная на всем $\mathbb{N}^2$ и сопоставляющая различным элементам $\mathbb{N}^2$ различные элементы $\mathbb{N}$.*

Доказательство. Эта функция сопоставляет паре $\langle n_1, n_2\rangle$ натуральное число, являющееся наименьшим кодом множества $\{n_1, n_1 + n_2\}$: значение этой функции на паре $\langle n_1, n_2\rangle$ равно k тогда и только тогда, когда $n_1 \in \tau(k)$, $n_1 + n_2 \in \tau(k)$, любое число, принадлежащее $\tau(k)$, равно n_1 или $n_1 + n_2$ и все числа, меньшие k, не обладают такими свойствами. Записывая сказанное в виде формулы языка арифметики, устанавливаем арифметичность построенной функции. То, что эта функция сопоставляет разным парам разные числа, легко следует из ее определения.

Теперь мы построим арифметическое кодирование конечных подмножеств $\mathbb{N}^2$ натуральными числами. А именно, числу k мы сопоставим подмножество $\mathbb{N}^2$, состоящее из тех пар $\langle x, y\rangle$, для которых число $v(x, y)$ принадлежит множеству $\tau(k)$. (Здесь v — функция из предыдущей леммы, τ — арифметическое кодирование конечных подмножеств $\mathbb{N}$ натуральными числами.) Легко видеть, что всякое конечное подмножество $\mathbb{N}^2$

поставлено в соответствие некоторому числу и множество

$$\{\langle k, x, y\rangle \mid \text{пара } \langle x, y\rangle \text{ принадлежит подмножеству } \mathbb{N}^2, \text{ соответствующему числу } k\}$$

является арифметическим подмножеством $\mathbb{N}^3$. (Эти требования мы и имели в виду, говоря о построении арифметического кодирования подмножеств $\mathbb{N}^2$.)

Теперь все готово для построения арифметического кодирования финитных функций одного аргумента элементами $\mathbb{N}^2$. Опишем, какая функция s ставится в соответствие паре натуральных чисел $\langle k, l\rangle$. Пусть A — подмножество $\mathbb{N}^2$, соответствующее k при арифметическом кодировании подмножеств $\mathbb{N}^2$. Если для данного числа x, меньшего или равного l, существуют такие y, для которых $\langle x, y\rangle \in A$, то $s(x)$ равно наименьшему из таких y; если таких y нет, то $s(x)=0$; при $x>l$ значение $s(x)$ равно 0. Всякой паре $\langle k, l\rangle$ соответствует финитная функция — функция, равная 0 на аргументах, бо́льших l. Чтобы найти код данной финитной функции s, надо в качестве l взять наибольшее число, на котором она отлична от 0, а в качестве k взять код множества $\{\langle x, y\rangle \mid x \leqslant l$ и $y = s(x)\}$. Записывая определение построенного кодирования в виде формулы языка арифметики, убеждаемся в его арифметичности.

Итак, для завершения доказательства существования арифметического кодирования финитных функций методом Смальяна осталось построить арифметическое кодирование конечных подмножеств $\mathbb{N}$. При этом построении мы будем использовать двоичную запись чисел, о которой можно прочесть, например, в уже упоминавшейся книжке О. Оре (Приглашение в теорию чисел. — М.: Наука, 1980).

Двоичная запись каждого натурального числа (кроме 0) начинается с 1; если мы условимся отбрасывать первую единицу, то получим взаимно однозначное соответствие между всеми положительными целыми числами и всеми словами в алфавите $\{0, 1\}$. Таким образом, инструкция «прибавь к числу 1, запиши его в двоичной системе и отбрось первую единицу» устанавливает взаимно однозначное соответствие между множеством натуральных чисел и мно-

жеством слов алфавита $\{0, 1\}$:

0	пустое слово
1	0
2	1
3	00
4	01
5	10
6	11
7	000
8	001
. . .	. . .

Слова в правой колонке расположены в порядке возрастания их длины, а слова одной длины расположены в словарном порядке. Число, стоящее в левой колонке, мы будем называть номером слова, стоящего в той же строке в правой колонке. При этой нумерации всякому множеству (двоичных) слов соответствует множество натуральных чисел. (Например, множеству слов, состоящих только из нулей, соответствует множество чисел, становящихся степенями двойки после прибавления 1.) Благодаря этому мы можем говорить об арифметичности множеств слов, имея в виду арифметичность соответствующих множеств натуральных чисел. Мы будем говорить также об арифметичности свойств слов, отождествляя свойство с множеством удовлетворяющих ему объектов. Аналогично определяются арифметические подмножества множества $(\{0, 1\}^{\infty})^n$, элементами которого являются последовательности из n слов; такие подмножества естественно отождествляются со свойствами последовательностей из n слов.

Установим теперь арифметичность некоторых конкретных свойств.

1° Слово X предшествует слову Y в упомянутом порядке. В самом деле, это имеет место тогда и только тогда, когда номер слова X меньше номера слова Y.

2° Слово X состоит из одних нулей.

В самом деле, в силу сказанного выше достаточно проверить арифметичность свойства «быть степенью двойки», а она, как объяснялось в приложении Б, вытекает из того, что число x тогда и только тогда является степенью двойки, когда всякий его делитель либо равен 1, либо четен.

3° Слово X состоит из одних единиц.

В самом деле, слово тогда и только тогда состоит из одних единиц, когда следующее за ним слово состоит из одних нулей.

4° Слово Y состоит из одних нулей и имеет ту же длину, что и слово X.

В самом деле, это равносильно тому, что слово Y — наибольшее в смысле рассмотренного порядка слово, состоящее из одних нулей и не превосходящее слова X.

5° Слова X и Y имеют одну и ту же длину. В самом деле, это равносильно тому, что существует слово Z, состоящее из одних нулей, имеющее одинаковую длину со словом X и со словом Y.

6° Слово X является соединением слов Y и Z, т. е. получается приписыванием слова Z к слову Y справа. $X = YZ$. Это, пожалуй, самый сложный пункт нашего рассуждения, в котором нам придется вспомнить о способе кодирования слов. Грубо говоря, арифметичность этого свойства вытекает из того, что для получения числа z, двоичная запись которого получается приписыванием друг к другу двоичных записей чисел x и y, необходимо умножить x на число $2^{(\text{длина } y)}$ и прибавить z. Следует, конечно, учесть, что при нашей нумерации слов мы прибавляем к числу единицу, а также не учитываем первую единицу двоичного разложения числа. Проделаем теперь все это подробнее. Пусть числа x, y и z являются номерами слов X, Y и Z. Это означает, что двоичная запись $x+1$ есть $1X$, двоичная запись $y+1$ есть $1Y$, а двоичная запись $z+1$ есть $1Z$. Пусть u — код слова, которое имеет ту же длину, что и Z, но состоит из одних нулей. Тогда двоичная запись числа $u+1$ будет иметь вид $1\underbrace{000\ldots0}_{\text{длина } Z}$. Если слово X является соединением слов Y и Z, то, умножая $y+1$ на $u+1$ и прибавляя $(z+1)-(u+1)$, мы получим число $x+1$. Из сказанного следует арифметичность интересующего нас свойства — искомой формулой будет запись на языке арифметики следующей фразы:

«существует u, являющееся кодом слова той же длины, что и Z, и состоящего из одних нулей, для которого $(y+1)\cdot(u+1)+(z-u)$ равно $x+1$».

Из арифметичности свойства «быть соединением» легко вывести арифметичность нескольких рассматриваемых дальше свойств.

7° Слово X является началом слова Y, т. е. существует такое слово Z, что Y является соединением X и Z.

8° Слово X является концом слова Y, т. е. существует такое слово Z, что Y есть соединение Z и X.

9° Слово X является подсловом (частью) слова Y. В самом деле, слово X тогда и только тогда является подсловом слова Y, когда оно является началом некоторого конца слова Y.

10° Слово X есть соединение слов Y, Z и V. В самом деле, слово X является соединением слов Y, Z и V тогда и только тогда, когда существует такое слово W, что W есть соединение Y и Z, а X — соединение W и V.

Аналогично может быть доказана арифметичность свойства «Y есть соединение $X_1, \ldots, X_n$» при любом фиксированном n.

Теперь мы можем построить арифметическое кодирование конечных множеств натуральными числами. Пусть x, y — натуральные числа, X, Y — соответствующие им слова. Пусть U — самое длинное слово из одних нулей, входящее в Y. Будем считать, что число x принадлежит множеству $\tau(y)$, если слово $1U1X1U1$ входит в Y. Докажем, что τ является кодированием конечных множеств. Пусть $\{x_1, \ldots, x_n\}$ — конечное множество чисел, $\{X_1, \ldots, X_n\}$ — множество соответствующих им слов. Пусть U — слово, состоящее из нулей и более длинное, чем любое из слов $X_1, \ldots$ $\ldots, X_n$. Обозначим через Y слово

$$1U1X_1 1U1X_2 1U1 \ldots 1U1X_n 1U1.$$

Номер слова Y и будет кодом множества $\{x_1, \ldots, x_n\}$. Арифметичность этого кодирования легко следует из арифметичности рассмотренных нами свойств слов. Построение кодирования методом Смальяна закончено.

Г. ЯЗЫКИ, СВЯЗАННЫЕ С АССОЦИАТИВНЫМИ ИСЧИСЛЕНИЯМИ

В этом приложении мы рассмотрим примеры языков с относительно просто устроенными множествами истинных утверждений. Эти примеры будут связаны с так называемыми ассоциативными исчислениями.

Ассоциативным исчислением в алфавите И называется произвольная конечная совокупность правил, разрешающих определенного вида преобразования слов в И. Эти правила называются двусторонними подстановками или (коль скоро мы не рассматриваем здесь односторонних подстановок) просто *подстановками* в алфавите И. Каждая подстановка в алфавите И записывается в виде

$$P \longleftrightarrow Q,$$

где P и Q суть слова в И, а буква $\longleftrightarrow$ не принадлежит алфавиту И. (Например, ци$\longleftrightarrow$цы есть подстановка в русском алфавите.) Подстановка $P \longleftrightarrow Q$ означает разрешение заменять слово P, если оно встретится как часть другого слова, на слово Q и обратно. Сказанное оформляется более точно в виде следующих определений. Для каждого ассоциативного исчисления (т. е. для каждого списка подстановок) вводится понятие смежных слов и эквивалентных слов. Два слова A и B называются *смежными* (записывается $A \perp B$), коль скоро существуют такие слова P, Q, X, Y, что: 1) $A = XPY$, 2) $B = XQY$ и 3) хотя бы одна из подстановок $P \longleftrightarrow Q$ и $Q \longleftrightarrow P$ есть подстановка рассматриваемого исчисления. Цепочку $\langle C_1, \ldots, C_n \rangle$ слов из $И^\infty$ назовем цепочкой смежности, если для каждого i имеет место $C_i \perp C_{i+1}$. Два слова A и B называются *эквивалентными*, коль скоро существует такая цепочка смежности $C_1, C_2, \ldots, C_n$, что $C_1 = A$, $C_n = B$.

Замечание 1. Если произвести факторизацию множества $И^\infty$ по так введенному отношению эквивалентности, получится алгебраическая система с ассоциативной операцией (возникающей при факторизации из операции приписывания друг к другу слов); отсюда и название — ассоциативное исчисление.

Пусть фиксировано некоторое ассоциативное исчисление в алфавите И. Существует алгоритм, позволяющий для каждых двух слов A и B из $И^\infty$ распознавать, смежны они или нет. Такой алгоритм состоит, например, в переборе всех четверок слов P, Q, X, Y, длина которых не превосходит длин A и B, и проверке условий 1), 2), 3). Таким образом, множество всех пар смежных слов разрешимо относительно $И^\infty \times И^\infty$. Однако существование алгоритма, распо-

знающего эквивалентность слов, очевидно лишь в простейших случаях.

Пример 1. Пусть $И = \{a, b, c\}$ и ассоциативное исчисление задано следующими подстановками:

$$ab \leftrightarrow ba,$$
$$ac \leftrightarrow ca,$$
$$bc \leftrightarrow cb.$$

Очевидно, что A и B эквивалентны тогда и только тогда, когда число букв a в слове A равно числу букв a в слове B, и то же самое выполняется для букв b и c. Такое исчисление естественно назвать *коммутативным*.

В общем случае не ясно, каким алгоритмом можно было бы обнаружить для произвольных слов, эквивалентны они или нет, т. е. имеется ли связывающая их цепочка смежных слов. И действительно, как показали А. А. Марков и Э. Л. Пост, возможно ассоциативное исчисление с неразрешимой проблемой распознавания эквивалентности (под проблемой распознавания эквивалентности как раз и понимается проблема отыскания алгоритма, распознающего эквивалентность слов). Доказательство существования таких исчислений приводится, например, в монографии С. К. Клини (Клини С. К. Введение в математику. — М.: ИЛ, 1957). Мы здесь приведем без доказательства следующий пример, принадлежащий Г. С. Цейтину.

Пример 2. Пусть $И = \{a, b, c, d, e\}$ и ассоциативное исчисление задано подстановками

$$ac \leftrightarrow ca,$$
$$ad \leftrightarrow da,$$
$$bc \leftrightarrow cb,$$
$$bd \leftrightarrow db$$
$$eca \leftrightarrow ce,$$
$$edb \leftrightarrow de,$$
$$cca \leftrightarrow ccae.$$

Как показал Г. С. Цейтин, для этого исчисления не существует алгоритма, распознающего эквивалентность слов.

Ассоциативное исчисление будем называть *разрешимым*, если для него существует алгоритм распозна-

вания эквивалентности; в противном случае будем называть его *неразрешимым*. Очевидно, что разрешимость ассоциативного исчисления равносильна разрешимости множества всех пар эквивалентных слов (и разрешимости множества всех пар неэквивалентных слов) относительно $И^{\infty} \times И^{\infty}$.

Фиксируем некоторое ассоциативное исчисление $\mathfrak{J}$ в алфавите И. Множество всех слов (в алфавите $И_{*}$) вида $A*B$, где $A \in И^{\infty}$, $B \in И^{\infty}$ и A эквивалентно (соответственно, неэквивалентно) B, обозначим через T^{+} (соответственно через T^{-}), так что $T^{+} \cup T^{-} = И^{\infty} \times И^{\infty}$. Тогда разрешимость исчисления $\mathfrak{J}$ означает разрешимость множества T^{+} (что равносильно разрешимости множества T^{-}) относительно $И^{\infty} \times И^{\infty}$

Замечание 2. Поэтому множество T^{+} (как и T^{-}), построенное для исчисления из примера 2, представляет собой индивидуальный пример неразрешимого подмножества множества $И^{\infty} \times И^{\infty}$. Характеристическая функция этого подмножества представляет собой в этом случае индивидуальный пример невычислимой функции.

С каждым ассоциативным исчислением в алфавите И мы свяжем теперь два языка — *позитивный язык*, утверждения которого будут утверждениями об эквивалентности произвольных двух слов в И, и *негативный язык*, утверждениями которого будут утверждения о неэквивалентности произвольных двух слов в И. В обоих случаях в качестве утверждений целесообразно рассматривать элементы множества $И^{\infty} \times И^{\infty}$ только в первом случае, для позитивного языка, слово $A*B$ будет интерпретироваться как утверждение об эквивалентности слов A и B, и потому множеством истинных утверждений будет служить T^{+}, тогда как во втором случае, для негативного языка, слово $A*B$ будет интерпретироваться как утверждение о неэквивалентности слов A и B, и потому множеством истинных утверждений будет служить T^{-}. Вспомним теперь, что в п. 1.3 § 1 мы договорились считать язык заданным, коль скоро указана соответствующая фундаментальная пара. Итак, пусть фиксирован алфавит И и ассоциативное исчисление $\mathfrak{J}$ в этом алфавите. Мы объявляем $\langle И_{*}, T^{+} \rangle$ фундаментальной парой позитивного языка, сопряженного с исчислением $\mathfrak{J}$, а $\langle И_{*}, T^{-} \rangle$ —

фундаментальной парой негативного языка, сопряженного с исчислением $\mathfrak{J}$.

Нас будет занимать вопрос о возможности ввести полную непротиворечивую дедуктику для $\langle И_*, T^+\rangle$ и для $\langle И_*, T^-\rangle$. Мы увидим, что в первом случае этот вопрос решается всегда положительно, а во втором — в зависимости от разрешимости исчисления $\mathfrak{J}$.

Лемма Г.1. *Множество E всех цепочек смежности разрешимо относительно $И_*^\infty$.*

Доказательство вытекает из существования алгоритма, распознающего смежность любых двух слов из $И^\infty$.

Теорема Г.1. *Для любого ассоциативного исчисления множество всех пар эквивалентных слов перечислимо.*

Доказательство. Введем на $И_*^\infty$ функцию φ, полагая

$$\varphi(C_1 * C_2 * \ldots * C_n) = C_1 * C_n$$

для каждого слова $C_1 * C_2 * \ldots * C_n$, где все C_i суть слова из $И^\infty$. Очевидно, что A и B эквивалентны тогда и только тогда, когда $A * B = \varphi(C)$ для некоторой цепочки смежности C. Поэтому $T^+ = \varphi(E)$, где E — множество всех цепочек смежности. Множество E разрешимо относительно $И_*^\infty$ (по лемме Г.1) и, следовательно, перечислимо (по лемме 2). Функция φ очевидным образом вычислима, а потому перечислимым будет и множество $\varphi(E)$. Но $\varphi(E) = T^+$, а перечислимость T^+ и надо было доказать.

Замечание 3. Таким образом, в случае неразрешимости исчисления T^+ будет служить примером перечислимого, но не разрешимого подмножества перечислимого множества $И^\infty \times И^\infty$. В силу леммы 3 всякий такой пример является одновременно примером перечислимого подмножества с неперечислимым дополнением. Ср. ниже замечание 5.

Следствие теоремы Г.1. *Для (фундаментальной пары) позитивного языка, сопряженного с произвольным ассоциативным исчислением, можно ввести полную непротиворечивую дедуктику.*

Замечание 4. Чтобы получить дедуктику, о которой говорится в этом следствии, нет нужды обращаться к теореме 1. Проще предъявить дедуктику $\langle И_*, E, \varphi\rangle$, где E и φ таковы, как в доказательстве

теоремы Г.1; она и будет полной непротиворечивой дедуктикой для $\langle И_*, T^+\rangle$. Эта дедуктика является совершенно естественной с содержательной точки зрения; в самом деле, лучшим доказательством эквивалентности слов A и B является предъявление связывающей их цепочки смежности.

Перейдем к вопросу о дедуктике для $\langle И_*, T^-\rangle$.

Теорема Г.2. *Пусть дано ассоциативное исчисление. Множество всех пар неэквивалентных слов тогда и только тогда перечислимо, когда это исчисление разрешимо.*

Доказательство. Заметим прежде всего, что $И^\infty \times И^\infty$ перечислимо (пример 6 из § 2). Пусть исчисление разрешимо; тогда T^- разрешимо относительно $И^\infty \times И^\infty$, а значит, само перечислимо (по лемме 2). Пусть теперь T^- перечислимо; поскольку его дополнение T^+ до перечислимого множества также перечислимо (по теореме Г.1), то в силу леммы 3 множество T^- разрешимо (относительно $И^\infty \times И^\infty$), а вместе с ним разрешимо и само рассматриваемое исчисление.

Замечание 5. Множество T^+, таким образом в случае неразрешимости исчисления служит примером перечислимого множества с неперечислимым дополнением (до некоторого объемлющего перечислимого множества); в силу леммы 3 всякий такой пример служит одновременно примером перечислимого множества, не являющегося разрешимым (опять-таки относительно некоторого перечислимого надмножества). Таким образом, существование перечислимого неразрешимого множества, доказанное нами в § 5, является следствием утверждения о существовании неразрешимых ассоциативных исчислений. Впрочем, обычные доказательства неразрешимости ассоциативных исчислений (в том числе исчисления из примера 2) как раз и опираются на существование перечислимого неразрешимого множества; этот факт, следовательно, подлежит сам доказательству, не опирающемуся на существование неразрешимых ассоциативных исчислений.

Следствие теоремы Г.2. *Для фундаментальной пары негативного языка, сопряженного с некоторым ассоциативным исчислением, тогда и только то-*

гда можно ввести полную непротиворечивую дедуктику, когда это исчисление разрешимо.

Введем теперь для произвольного ассоциативного исчисления $\mathfrak{J}$ в алфавите И *универсальный язык*, утверждениями которого будут служить как утверждения об эквивалентности слов, так и утверждения о неэквивалентности. Здесь нам придется отличать первые утверждения от вторых. С этой целью пополним алфавит И еще одной буквой, буквой $\urcorner$, в предположении, что она, как и $\longleftrightarrow$ и $*$, не входит в И. Алфавит И $\cup \langle *, \urcorner \rangle$ обозначим через Л. Обозначим через $\urcorner T^-$ множество всех слов вида $\urcorner P$, где $P \in T^-$. Положим $T^0 = T^+ \cup \urcorner T^-$ и образуем фундаментальную пару $\langle Л, T^0 \rangle$. Элемент t из T^0 естественно интерпретировать как истинное утверждение об эквивалентности слов (если $t \in T^+$) или о неэквивалентности слов (если $t \in \urcorner T^-$).

Теорема Г.3. *Для любого ассоциативного исчисления $\mathfrak{J}$ соответствующее ему множество T^0 тогда и только тогда перечислимо, когда исчисление разрешимо.*

Доказательство. Если $\mathfrak{J}$ разрешимо, то T^- перечислимо (теорема Г.2), а потому перечислимо и $\urcorner T^-$ (пример 5 из § 2). Тогда T^0 перечислимо по лемме 5. Пусть теперь перечислимо T^0. Образуем множество $\urcorner Л^\infty$ всех слов в алфавите Л, начинающихся с $\urcorner$; это множество перечислимо (примеры 2 и 5 из § 2). По лемме 5 перечислимо пересечение $T^0 \cap \urcorner Л^\infty$ Но $T^0 \cap \urcorner Л^\infty = \urcorner T^-$. Поэтому перечислимо $\urcorner T^-$, а вместе с ним и T^- (пример 5 из § 2); но тогда по теореме Г.2 разрешимо исчисление $\mathfrak{J}$.

Следствие. *Для фундаментальной пары универсального языка, сопряженного с некоторым ассоциативным исчислением, тогда и только тогда можно ввести полную непротиворечивую дедуктику, когда это исчисление разрешимо.*

Д. ИСТОРИЧЕСКИЕ ЗАМЕЧАНИЯ

Один из наиболее выдающихся математиков XX века (и, безусловно, самый выдающийся математический логик) Курт Гёдель (Kurt Gödel) родился 28 апреля 1906 года в городе Брно (ныне Чехословакия, тогда Австро-Венгрия). С 40-х годов Гёдель работал в

Принстоне (США), где и умер 14 января 1978 года. С именем Гёделя связаны важнейшие теоремы математической логики: теорема о полноте исчисления предикатов (1930 г.), теорема о неполноте арифметики (1930 г.), теорема о непротиворечивости аксиомы выбора и континуум-гипотезы (1938 г.).

Теорема о полноте исчисления предикатов утверждает, что можно предложить полную и непротиворечивую дедуктику для языка логики предикатов, а точнее — что некоторая конкретная (и ранее известная) дедуктика такова; таким образом, в этой дедуктике можно доказать все истины логики предикатов, т. е. всякую формулу, выражающую «закон логики» (и нельзя доказать никакие иные формулы). (Под «законом логики» понимается формула, истинность которой сохраняется при *любом* истолковании участвующих в ней имен.) Теорема о неполноте (ей и посвящена настоящая брошюра), напротив, утверждает, что подобная ситуация невозможна в случае арифметики: не только известные дедуктики не являются одновременно полными и непротиворечивыми, но такая дедуктика в принципе невозможна; как было разъяснено выше в основном тексте брошюры, ни при каком понятии формального доказательства не удается доказать все истины арифметики и только их. Ниже будет приведена формулировка теоремы о неполноте в той форме, как она была высказана самим Гёделем. Теорема о непротиворечивости аксиомы выбора и аксиомы, выражающей континуум-гипотезу, гласит, что теория множеств остается непротиворечивой после присоединения указанных двух аксиом, коль скоро она была непротиворечивой до такого присоединения. Этот результат Гёделя — первый фундаментальный результат, относящийся к исследованию непротиворечивости теоретико-множественных утверждений, — в значительной степени изменил наши представления о смысле этих утверждений и положил начало новому направлению в математической логике.

О названных теоремах Гёделя можно прочесть в книгах, указанных в предисловии. Гёделю принадлежит и много других важных понятий и результатов [в частности первое (1934 г.) определение понятия рекурсивной функции: рекурсивность по Эрбрану — Гёделю]; всех их невозможно здесь перечислить. Мы

сейчас остановимся подробнее на первоначальной гёделевой формулировке теоремы о неполноте.

Знаменитая работа Курта Гёделя «Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I» («О формально неразрешимых предложениях Principia Mathematica [1]) и родственных систем I») была напечатана на с. 173—198 1-й тетради 38-го тома (за 1931 г.) лейпцигского журнала «Monatshefte für Mathematik und Physik» (поступила 17/XI 1930). Предварительная сводка результатов была опубликована в венском журнале Anzeiger der Akademia der Wissenschaften in Wien, Mathematisch-naturwissenschaftliche Klasse, № 19 за 1930 г. (заседание от 23 октября 1930 г.).

В этой статье для широкого класса формальных систем устанавливалось неизбежное существование в каждой из таких систем неразрешимого утверждения — неразрешимого в том смысле, что ни оно, ни его отрицание не могло быть выведено из аксиом системы. Именно, в статье Гёделя была сформулирована следующая теорема (теорема VI на с. 187):

Для каждого ω-непротиворечивого рекурсивного класса *κ формул* существует такая рекурсивная *классовая формула r*, что ни *v* Gen *r*, ни Neg(*v* Gen *r*) не принадлежит к Flg(*κ*) (где *v* есть *свободная переменная формулы r*).

Дадим некоторые пояснения к приведенным формулировкам. Эти пояснения предполагают наличие у читателя простейших сведений из математической логики.

Речь здесь идет о формулах некоторой формальной системы *P*, которая строится на страницах 176—178 статьи Гёделя. Мы не будем приводить точных формулировок, а ограничимся следующей цитатой из Гёделя: «В сущности, *P* есть та система, которая получается, если надстроить пеановские аксиомы логикой Principia Mathematica (числа в качестве индивидов, отношение «следования за» в качестве неопределяемого понятия)» (с. 176). Курсив несет на себе определенный смысл. Он означает, что речь идет не непосредственно о знакосочетаниях рассматриваемой формальной системы (переменных, формулах и т. п.),

[1]) Имеется в виду монография: Whitehead A., Russell B. Principia Mathematica. — 2-е изд. — Cambridge, 1925.

а о номерах этих знакосочетаний в некоторой фиксированной нумерации (называемой теперь гёделевской). Классовая формула — это формула с одной свободной переменной. Стало быть, *классовая формула* — это натуральное число, являющееся номером классовой формулы. Через $v\,\mathrm{Gen}\,r$ обозначается номер формулы, полученной навешиванием квантора общности по переменной с номером v на формулу с номером r; через $\mathrm{Neg}(v\,\mathrm{Gen}\,r)$ — номер отрицания предыдущей формулы. Через $\mathrm{Flg}(\varkappa)$ обозначается класс номеров всех тех и только тех формул, которые выводимы из класса формул, номера которых образуют класс $\varkappa$[1]). Термины «рекурсивный класс» и «рекурсивная формула» мы оставим без объяснений; эти термины означают некоторую определимость рассматриваемых классов и формул с помощью примитивно рекурсивных функций (в статье Гёделя такие функции называются просто «рекурсивными»). Свойство ω-непротиворечивости, налагаемое на класс, означает условие более сильное, нежели простая непротиворечивость[2]). Если непротиворечивость класса означает невозможность вывести из него как некоторую формулу, так и ее отрицание, то ω-непротиворечивость означает невозможность вывести как некоторую формулу вида «существует такое x, что $\mathfrak{A}(x)$», так и все формулы вида «не $\mathfrak{A}(0)$», «не $\mathfrak{A}(1)$», «не $\mathfrak{A}(2)$» и т. д. В обозначениях обсуждаемой статьи Гёделя класс $\varkappa$ *формул* (т. е. номеров формул) называется ω-непротиворечивым, если не существует *классовой формулы* a, для которой: 1) $\mathrm{Neg}(v\,\mathrm{Gen}\,a) \in \mathrm{Flg}(\varkappa)$, 2) $\mathrm{Sb}\left(a^{v}_{Z(n)}\right) \in \mathrm{Flg}(\varkappa)$ при всех n (здесь $\mathrm{Sb}\left(a^{v}_{Z(n)}\right)$ означает номер результата подстановки в формулу с номером a формулы с номером $Z(n)$ вместо переменной с номером v, причем $Z(n)$ — номер выражения для числа n). Таким образом, теорема VI гласит, что для любого класса формул, подчиненного некоторым условиям, существует формула сравнительно простого

[1]) Вывод из произвольного класса формул предполагает возможность использовать в процессе вывода также и аксиомы, так что в данном случае происходит присоединение класса $\varkappa$ к аксиомам исходной системы.

[2]) Впоследствии Россер усилил первоначальную формулировку Гёделя, заменив требование ω-непротиворечивости более слабым требованием непротиворечивости.

вида такая, что ни она, ни ее отрицание невыводимы из этого класса. Поскольку в основе формальной системы P, подразумеваемой в названной теореме (ведь речь идет о формулах этой системы и о выводимости по правилам этой системы), лежат арифметические аксиомы Пеано, то сама эта теорема часто интерпретируется как теорема о неполноте формальной арифметики. Неполнота понимается здесь в синтаксическом смысле (см. приложение А).

Замечание 1. Если под формальной арифметикой понимать систему P, то неполнота формальной арифметики представляет собой весьма частный случай теоремы VI, получающийся при $\varkappa = \varnothing$ (и справедливый в предположении, что сама P является ω-непротиворечивой, т. е. что ω-непротиворечив класс ее аксиом); в этом случае $\mathrm{Flg}(\varkappa)$ состоит просто из номеров всех формул, доказуемых в P.

Замечание 2. Правда, сама неразрешимая формула, указываемая в теореме VI, а именно, формула с номером $v\,\mathrm{Gen}\,r$, еще не имеет арифметического характера, т. е. еще не записана на простейшем арифметическом языке. Однако на этот счет в статье Гёделя содержатся важные дальнейшие результаты. Именно, формула называется «арифметической», если она строится с помощью переменных, пробегающих натуральный ряд, отношения равенства и операций сложения и умножения[1]). Далее, на с. 193 статьи Гёделя формулируется теорема VIII:

В каждой формальной системе, упоминаемой в теореме VI, существуют неразрешимые арифметические утверждения.

Замечание 3. Как указывает Гёдель (с. 190), его доказательство теоремы VI проходит не только для конкретной системы P, о которой идет речь в его статье, но для любой системы, обладающей следующими основными свойствами:

---

[1]) Заметим, что знаки $=$, $+$, $\cdot$ не входят в исходный алфавит системы P. Поэтому «арифметическая формула» может существовать лишь в подходящем расширении системы P. В рамках же P эти знаки следует рассматривать как сокращающие. Так, выражение $x_1 = y_1$ понимается, согласно подстрочному примечанию 21 на с. 177, как сокращение для формулы «$x_2\Pi(x_2(x_1) \supset \supset x_2(y_1))$»; здесь $x_2\Pi$ означает квантор общности по x_2. (Для $x + y$ и $x - y$ такие расшифровки в статье Гёделя не приводятся.)

1) аксиомы и правила вывода системы рекурсивно определимы;

2) каждое рекурсивное отношение определимо внутри системы.

Как отмечает Гёдель, эти свойства выполняются для аксиоматических систем теории множеств Цермело — Френкеля и фон Неймана, а также для аксиоматической теории чисел, основанной на аксиомах Пеано и рекурсивных определениях. Во всех этих системах существуют, следовательно, неразрешимые предложения: чтобы обнаружить это, достаточно положить $\varkappa = \varnothing$ (ср. выше замечание 1). Правда, утверждение предыдущей фразы справедливо лишь в предположении ω-непротиворечивости рассматриваемой системы. Это предположение во всех конкретных случаях образует рабочую гипотезу, вытекающую из нашего убеждения в разумности рассматриваемой системы, т. е. в том, что она адекватно отражает некоторую реальность.

Е. УПРАЖНЕНИЯ

В этом приложении приведены упражнения к некоторым разделам брошюры. Более трудные из них помечены звездочкой.

Упражнения к § 2.

1. Пересечение и объединение двух разрешимых подмножеств некоторого множества являются разрешимыми подмножествами этого множества.

2. Пересечение и объединение двух перечислимых множеств перечислимы.

3. Если график функции перечислим, то функция вычислима. (Обратное утверждение доказывается в § 5.)

4. Если $A \subset \mathbb{N}$ разрешимо (перечислимо), то $\{x \mid 2x \in A\}$ разрешимо (перечислимо).

5. Если $A \subset \mathbb{N}$ перечислимо, то $B = \{x \mid \exists k \in \mathbb{N} (kx \in A)\}$ перечислимо. (Даже если A разрешимо, B может быть неразрешимым, см. упражнение 16 к § 5.)

6. Множество $\mathbb{N}^3$ всех троек натуральных чисел перечислимо.

7. Множество $A \subset \mathbb{N}$ перечислимо тогда и только тогда, когда оно является проекцией некоторого разрешимого множества $R \subset \mathbb{N}^2$.

8. Если A — разрешимое подмножество B, а C — разрешимое подмножество D, то $A \times C$ — разрешимое подмножество $B \times D$.

9. Любое бесконечное перечислимое множество P может быть перечислено вычислимой функцией без повторений: существует такая вычислимая функция p, определенная на всем $\mathbb{N}$, что $P = \{p(0), p(1), \ldots\}$ и $p(n) \neq p(m)$ при $n \neq m$.

10. Пусть A — множество натуральных чисел. *Прямым пересчетом* A называется функция, сопоставляющая числу 0 наименьший элемент A, числу 1 — следующий по величине элемент A и т. д. (Если A конечно, прямой пересчет A не всюду определен.) Множество A является разрешимым подмножеством $\mathbb{N}$ тогда и только тогда, когда его прямой пересчет является вычислимой функцией.

11. Бесконечное перечислимое подмножество $P \subset \subset \mathbb{N}$ всегда имеет бесконечное подмножество, являющееся разрешимым подмножеством $\mathbb{N}$.

12. Пусть A и B — пересекающиеся перечислимые множества. Тогда существуют такие перечислимые множества A_1 и B_1, что $A \cup B = A_1 \cup B_1$, $A_1 \cap B_1 = \varnothing$, $A_1 \subset A$, $B_1 \subset B$.

13. Пусть P — перечислимое подмножество $\mathbb{N}^2$. Тогда существует вычислимая функция f из $\mathbb{N}$ в $\mathbb{N}$, определенная на всех тех x, для которых $\langle x, y \rangle \in P$ при некотором y, значение которой есть один из таких y (т. е. $\langle x, f(x) \rangle \in P$ для всех x, на которых f определена).

14. Выведите утверждение задачи 12 из утверждения задачи 13.

15. Назовем множество A натуральных чисел *вычислимо бесконечным*, если существует алгоритм, который по n дает список более чем из n различных элементов A. Следующие свойства равносильны:

1° A вычислимо бесконечно;

2° A содержит бесконечное перечислимое подмножество;

3° A содержит бесконечное подмножество, являющееся разрешимым подмножеством $\mathbb{N}$;

4° существует такая вычислимая функция из $\mathbb{N}$ в $\mathbb{N}$, определенная на всех натуральных числах, что для всех n верно $f(n) \in A$ и $f(n) \geqslant n$.

16*. Существует бесконечное множество, не являющееся вычислимо бесконечным.

17. Функция f, определяемая так: $f(n) = 1$, если в десятичном разложении числа π имеется по крайней мере n идущих подряд девяток, $f(n) = 0$ в противном случае, вычислима. (Если вместо «по крайней мере» в предыдущей фразе написать «ровно», то ответ на вопрос о вычислимости получающейся функции неизвестен.)

18*. Является ли разрешимым подмножеством $\mathbb{N}^2$ множество таких пар $\langle m, n \rangle$ натуральных чисел, для которых $n \neq 0$ и $m/n < e$? (Число e — основание натуральных логарифмов.)

19*. Является ли вычислимой функция, сопоставляющая числу n стоящий на n-м месте знак десятичного разложения числа e?

20. Следующие условия на действительное число x равносильны:

1° существует алгоритм, дающий по n числа p и q, для которых $q \neq 0$ и $|p/q - x| < 1/n$;

2° множество $\{\langle p, q \rangle \mid q \neq 0$ и $p/q < x\}$ разрешимо;

3° функция, сопоставляющая числу n стоящий на n-м месте знак десятичного разложения числа x, вычислима. Если эти условия выполнены, то число x называют *вычислимым* действительным числом.

21*. (Продолжение.) Сумма, произведение и частное вычислимых действительных чисел вычислимы. Всякий корень целочисленного многочлена вычислим.

22. (Продолжение.) Существуют невычислимые действительные числа.

Упражнения к § 3.

1. Будем говорить, что всюду определенная функция из $К^\infty$ в $Л^\infty$ *сводит* множество $A \subset К^\infty$ к множеству $B \subset Л^\infty$, если для всех $x \in К^\infty$ условия $x \in A$ и $f(x) \in B$ равносильны. (Мы «сводим» задачу выяснения принадлежности x к A к задаче выяснения принадлежности $f(x)$ к B.) Если B разрешимо (перечислимо) и A сводится к B некоторой вычислимой функцией, то A разрешимо (перечислимо).

2. (Продолжение.) Если A сводится к B некоторой вычислимой функцией и A неразрешимо (неперечислимо), то B неразрешимо (неперечислимо).

3. (Продолжение.) Множество $X \subset \mathbb{N}$ тогда и только тогда выразимо посредством фундаментальной пары $\langle Б, T \rangle$, когда оно сводится к множеству T некоторой вычислимой функцией.

4. Будем говорить, что множества натуральных чисел A и B *равны почти всюду*, если их разности $A \setminus B$ и $B \setminus A$ конечны. Множество, почти всюду равное разрешимому, разрешимо. Множество, почти всюду равное перечислимому, перечислимо.

Упражнения к § 4.

1. Добавив в язык арифметики новый квантор $\forall_ч$, который означает «для всех четных»: $\forall_ч \xi \alpha$ истинно, если для всех четных n суждение $S_n^\xi \alpha$ истинно. От этого добавления класс арифметических множеств не изменится.

2. Пусть α, β, γ — любые суждения. Следующие суждения истинны:

а) $(\alpha \wedge (\alpha \to \beta)) \to \beta$;

б) $(\alpha \wedge (\beta \vee \gamma)) \leftrightarrow ((\alpha \wedge \beta) \vee (\alpha \wedge \gamma))$;

в) $(\alpha \to (\beta \to \gamma)) \leftrightarrow ((\alpha \wedge \beta) \to \gamma)$;

г) $((\alpha \to \gamma) \wedge (\beta \to \gamma)) \leftrightarrow (\alpha \vee \beta \to \gamma)$;

д) $(((\alpha \to \beta) \to \alpha) \to \alpha)$;

е) $\neg (\alpha \wedge \beta) \leftrightarrow (\neg \alpha \vee \neg \beta)$;

ж) $\neg (\alpha \vee \beta) \leftrightarrow (\neg \alpha \wedge \neg \beta)$;

з) $((\alpha \to \beta) \wedge (\alpha \to \neg \beta)) \to \neg \alpha$;

и) $(\alpha \wedge \neg \alpha) \to \beta$;

к) $(\alpha \to \beta) \leftrightarrow (\neg \alpha \vee \beta)$;

л) $(\alpha \leftrightarrow \beta) \leftrightarrow ((\alpha \to \beta) \wedge (\beta \to \alpha))$;

м) $(\alpha \vee \beta) \leftrightarrow \neg (\neg \alpha \wedge \neg \beta)$.

3. Пусть α — формула, не имеющая отличных от ξ параметров. Тогда следующие суждения истинны:

а) $\forall \xi \alpha \to \exists \xi \alpha$;

б) $\neg \forall \xi \alpha \leftrightarrow \exists \xi \neg \alpha$;

в) $\neg \exists \xi \alpha \leftrightarrow \forall \xi \neg \alpha$.

4. Исключим из языка арифметики $\vee$, $\to$, $\leftrightarrow$, $\exists$ (останутся $\neg$, $\wedge$, $\forall$). Класс арифметических множеств не изменится.

5. Множества

$$\{x \mid x \text{ делится на } 3\},$$

$$\{x \mid x \text{ есть степень числа } 3\},$$

$$\{x \mid \text{последняя цифра десятичной записи } x \text{ есть } 7\}$$

арифметичны.

6*. Множество $\{x \mid x \text{ есть степень числа } 10\}$ арифметично.

7. Всякое арифметическое множество сопряжено с формулой, в которую не входят цифры.

8. Существует неарифметическое множество.

Упражнения к § 5.

1. Следующие свойства равносильны: а) X — перечислимое множество; б) X — область определения некоторой вычислимой функции; в) X — область значений некоторой вычислимой функции.

2. Для всякой вычислимой функции f существует вычислимая функция g, обладающая следующим свойством: $g(y)$ определено в том и только том случае, когда y принадлежит множеству значений f; в этом случае $f(g(y)) = y$.

3. Если f — вычислимая функция из $\mathbb{N}$ в $\mathbb{N}$, то множество $\{x \mid f(x) = 1981\}$ перечислимо.

4. Не существует функции из $\mathbb{N}^2$ в $\mathbb{N}$, универсальной для класса всех всюду определенных функций из $\mathbb{N}$ в $\mathbb{N}$.

5. Не существует функции из $\mathbb{N}^2$ в $\mathbb{N}$, универсальной для класса всех функций из $\mathbb{N}$ в $\mathbb{N}$.

6. Пусть α — функция, от которой никакая вычислимая функция не может всюду отличаться. Тогда множество $\{x \mid \alpha(x) = 1981\}$ перечислимо и неразрешимо.

7. Существует неперечислимое множество с неперечислимым дополнением. Это множество может быть выбрано арифметическим.

8. Пусть F — вычислимая функция из $\mathbb{N}^2$ в $\mathbb{N}$. Будем говорить, что число n является *номером* функции F_n относительно F. Будем говорить, что нумера-

ция, задаваемая функцией F', *сводится* к нумерации, задаваемой функцией F, если существует вычислимая всюду определенная функция h из $\mathbb{N}$ в $\mathbb{N}$, дающая по F'-номеру некоторой функции F-номер той же функции: $F_{h(n)} = F'_n$. Существует такая функция F из $\mathbb{N}^2$ в $\mathbb{N}$, что для всякой функции F' из $\mathbb{N}^2$ в $\mathbb{N}$ нумерация, задаваемая F', сводится к нумерации, задаваемой функцией F. Функции с этим свойством необходимо являются универсальными. Они называются *главными* универсальными функциями.

9. Пусть F — вычислимая функция из $\mathbb{N}^2$ в $\mathbb{N}$. Множества $\{n \mid F_n$ где-то определена$\}$ и $\{n \mid F_n$ принимает значение 1980$\}$ перечислимы.

10. Для некоторой вычислимой функции F из $\mathbb{N}^2$ в $\mathbb{N}$ множество $\{n \mid F_n$ где-то определена$\}$ является перечислимым множеством с неперечислимым дополнением.

11. Существует перечислимое множество $P \subset \mathbb{N}^2$, у которого множество нижних точек, т. е. множество

$$\{\langle x, y\rangle \mid \langle x, y\rangle \in P \text{ и } \forall y' < y\, (\langle x, y'\rangle \notin P)\},$$

неперечислимо.

12. Пусть P — подмножество $\mathbb{N} \times \mathbb{N}$. Обозначим через P_n множество $\{x \in \mathbb{N} \mid \langle n, x\rangle \in P\}$. Если P перечислимо, то все P_n перечислимы. Существует такое перечислимое P, что среди P_n встречаются все перечислимые подмножества $\mathbb{N}$. Такие P называются *универсальными* для класса перечислимых подмножеств $\mathbb{N}$ перечислимыми множествами.

13. (Продолжение.) Если P — универсальное для класса перечислимых подмножеств $\mathbb{N}$ перечислимое множество, то

$$\{x \mid \langle x, x\rangle \notin P\} \text{ неперечислимо},$$

и, следовательно,

$$\{x \mid \langle x, x\rangle \in P\} \text{ — перечислимое множество с неперечислимым дополнением.}$$

14. Не существует такого разрешимого подмножества R множества $\mathbb{N}^2$, чтобы среди его сечений $R_n = \{x \in \mathbb{N} \mid \langle n, x\rangle \in R\}$ встречались все разрешимые подмножества $\mathbb{N}$.

15*. Существует перечислимое множество натуральных чисел, дополнение которого бесконечно, но не содержит бесконечного перечислимого подмножества (т. е. не вычислимо бесконечно).

16. Существует такое разрешимое подмножество R множества $\mathbb{N}$, что множество $\{x \mid \exists k \in \mathbb{N} (kx \in R)\}$ неразрешимо.

Упражнения к приложению А.

1. Если A и B неотделимы, то A и B неразрешимы.

2. Существуют три попарно непересекающихся перечислимых множества A, B, C, любые два из которых неотделимы.

3. Если A и B — перечислимые подмножества $\mathbb{N}$ и $A \cup B = \mathbb{N}$, то $A \setminus B$ и $B \setminus A$ отделимы.

4. Существуют такие множества $A, B \subset \mathbb{N}$, что никакое арифметическое множество не отделяет A от B.

Упражнения к приложению Б.

1. Проекция арифметического множества на любые оси в смысле § 2 арифметична.

2. Композиция арифметических функций арифметична. Если арифметическая функция имеет обратную, то обратная к ней функция арифметична.

3. Всякая арифметическая функция из $\mathbb{N}$ в $\mathbb{N}$ имеет арифметическое всюду определенное продолжение.

4. Арифметические множества — наименьший класс, содержащий множества из примера 6 приложения Б и удовлетворяющий леммам Б.1—Б.4.

5*. Определим кванторную глубину формулы так: кванторная глубина элементарных формул равна 0; кванторная глубина формулы $\neg\alpha$ равна кванторной глубине формулы α; кванторная глубина формул $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$, $(\alpha \leftrightarrow \beta)$ равна максимуму из кванторных глубин формул α и β; кванторная глубина формул $\exists\xi\alpha$ и $\forall\xi\alpha$ на 1 больше кванторной глубины формулы α. Для каждого натурального k множество истинных суждений языка арифметики, кванторная глубина которых не превосходит k, арифметично.

6*. При любой нумерации суждений языка арифметики и любой нумерации классовых формул множества $\{n \mid n\text{-е суждение истинно}\}$ и $\{\langle m, n, k\rangle \mid k$ есть

номер суждения, получающегося в результате подстановки n вместо x_1 в m-ю классовую формулу} не могут быть одновременно арифметичными.

Упражнения к приложению В.

1. Следующие функции адресно вычислимы:
а) $f(x) = 2^x$;
б) $f(x, y) = x^y$;
в) $f(x) = x$-е простое число;
г) $f(x) =$ сумма цифр десятичной записи x;
д)* $f(x) = x$-я цифра в десятичной записи числа e.

2*. Класс адресно вычислимых функций из $\mathbb{N}$ в $\mathbb{N}$ не изменился бы, если бы мы ограничились некоторым фиксированным числом регистров, например запретили бы употреблять в адресных программах регистры с номерами, бо́льшими 100.

3. Класс адресно вычислимых функций не расширился бы, если бы мы ввели команды с косвенной адресацией, т. е. команды вида $R(a) \leftarrow R(R(b))$ и $R(R(b)) \leftarrow R(a)$, согласно которым содержимое регистра с номером, равным содержимому регистра $R(b)$, пересылается в a-й регистр и наоборот.

4. Следующие множества являются слабо аналитическими:
а) $\{\langle x, y, z\rangle \mid z = x^y\}$;
б) $\{\langle x, y\rangle \mid x$ есть y-е простое число$\}$.

5. Всякое слабо аналитическое множество является аналитическим (показать, не используя теоремы об арифметичности слабо аналитических множеств).

6*. Множество номеров истинных суждений языка арифметики при любой вычислимой нумерации слов из A^∞ аналитично.

7*. Класс аналитических множеств не изменится, если из расширенного языка арифметики исключить двуместные функциональные переменные.

8*. Множество суждений расширенного языка арифметики, истинных в том случае, когда допустимыми считаются все функции, не аналитично. Множество суждений расширенного языка арифметики, истинных в том случае, когда допустимыми считаются лишь финитные функции, аналитично.

9*. Назовем множество $P \subset \mathbb{N}^k$ *адресно перечислимым*, если оно пусто или если существуют такие адресно вычислимые функции $g_1, \ldots, g_k$ из $\mathbb{N}$ в $\mathbb{N}$,

определенные на всем $\mathbb{N}$, что $P = \{\langle g_1(n) \ldots$ $\ldots g_k(n)\rangle \mid n \in \mathbb{N}\}$. График адресно вычислимой функции адресно перечислим (доказать без использования аксиомы протокола).

10*. Существует адресно вычислимая функция из $\mathbb{N}^2$ в $\mathbb{N}$, универсальная для класса адресно вычислимых функций из $\mathbb{N}$ в $\mathbb{N}$ (доказать без использования аксиомы программы).

Упражнения к приложению Г.

1. Пусть И $= \{a, b\}$ и ассоциативное исчисление задано подстановками:

$$a \leftrightarrow aa,$$

$$b \leftrightarrow bb.$$

Будет ли оно разрешимо?

2. Доказать, что любое ассоциативное исчисление в однобуквенном алфавите разрешимо.

3. Ассоциативные исчисления являются примерами *исчислений*. Понятие исчисления, пожалуй, столь же фундаментально, как и понятие алгоритма. Главное отличие исчислений от алгоритмов состоит в том, что исчисление разрешает какие-то действия, в то время как алгоритм предписывает их. Если заменить двусторонние подстановки односторонними (разрешить заменять левую часть на правую, но не наоборот), сформулировать правило, определяющее, какую подстановку и в каком месте слова надлежит применять, а также определить, когда переработка слова считается законченной, то от исчислений мы перейдем к алгоритмам (именно так получаются нормальные алгоритмы, с помощью которых А. А. Марков доказал существование неразрешимых ассоциативных исчислений). В настоящем упражнении мы рассмотрим отчасти сходный пример алгоритма. Этот алгоритм применяется к словам в алфавите $\{a, b\}$ и состоит в следующем:

1. Если слово начинается на a, т. е. имеет вид aP, где P — некоторое слово, то его надо преобразовать в Pb.

2. Если слово имеет вид baP, то его надо преобразовать в $Paba$.

3. Эти преобразования надо повторять до тех пор, пока не получится слово вида aaP. После этого при-

менение алгоритма заканчивается и результатом будет P.

Что произойдет, если применить описанный алгоритм к словам *babaa*, *baaba* и *abaab*?

4. Построить разрешающий алгоритм для ассоциативного исчисления в алфавите $\{a, b, c\}$, заданного следующими подстановками:

$$b \leftrightarrow acc,$$
$$ca \leftrightarrow accc,$$
$$aa \leftrightarrow,$$
$$bb \leftrightarrow,$$
$$cccc \leftrightarrow.$$

(В правой части трех последних подстановок стоят пустые слова.)

Е. ОТВЕТЫ И УКАЗАНИЯ К УПРАЖНЕНИЯМ

В этом приложении приведены ответы и указания к некоторым из упражнений приложения Е. Номер упражнения указывается так: 4.7 означает седьмое упражнение к § 4, а Б.3 — третье упражнение к приложению Б.

2.2. См. § 3.

2.3. Если график f равен $\{\langle p(n), q(n)\rangle \mid n \in \mathbb{N}\}$, то $f(x) = q$ (наименьшее из тех n, для которых $p(n) = x$).

2.4. Ср. лемму 6 из § 3.

2.5. Если $A = \{f(n) \mid n \in \mathbb{N}\}$, $b \in B$, то B есть образ $\mathbb{N}^3$ при функции g:

$$g(k, l, n) = \begin{cases} l, & \text{если} \quad kl = f(n), \\ b & \text{в противном случае.} \end{cases}$$

2.6. Ср. следствие 1 леммы 4.

2.7. Если $A = \{f(n) \mid n \in \mathbb{N}\}$, то A есть проекция множества $R = \{\langle f(n), n\rangle \mid n \in \mathbb{N}\}$.

2.9. Пусть функция f перечисляет множество P. Искомая последовательность $p(0), p(1), \ldots$ получается из последовательности $f(0), f(1), \ldots$ вычеркиванием повторений, т. е. тех членов $f(n)$, для которых $f(n) = f(k)$ при некотором $k < n$.

2.11. Воспользовавшись 2.9, представим P как $\{p(0), p(1), \ldots\}$, выберем вычислимую монотонно воз-

растающую подпоследовательность (отбросив члены, меньшие предыдущих) и применим 2.10.

2.12. Зафиксируем перечисления a и b множеств A и B: $A = \{a(i) \mid i \in \mathbb{N}\}$, $B = \{b(i) \mid i \in \mathbb{N}\}$. Рассмотрим последовательность $a(0)$, $b(0)$, $a(1)$, $b(1)$, ... Те числа, которые впервые появляются на четных местах этой последовательности, отнесем к A_1. Те числа, которые впервые появляются на нечетных местах этой последовательности, отнесем к B_1.

2.13. Зафиксируем перечисление множества P. Тогда значение функции f на числе x будет равно тому y, для которого пара $\langle x, y\rangle$ появляется в перечислении множества P раньше всех других пар вида $\langle x, z\rangle$ (пар, первым членом которых является x).

2.14. Рассмотрим в $\mathbb{N}^2$ множество $(A \times \{0\}) \cup \cup (B \times \{1\})$ и применим 2.13.

2.15. При доказательстве $2° \Rightarrow 3°$ применяется 2.11.

2.16. Будем строить множество I, не содержащее ни одного бесконечного перечислимого подмножества (ср. 2.15). Семейство всех бесконечных перечислимых подмножеств счетно. Пусть $W_0, W_1, \ldots$ — все такие множества. Мы будем строить наше множество I по шагам, добиваясь на i-м шаге того, чтобы W_i не было подмножеством I и чтобы I содержало по крайней мере i элементов. На нулевом шаге мы обеспечим выполнение условия $W_0 \not\subset I$, выбрав в W_0 какой-то элемент a_0 и условившись, что a_0 не принадлежит I. На i-м шаге мы обеспечим выполнение условия $W_i \not\subset I$, выбрав в W_i элемент a_i, который мы еще не условились включать в I (это можно сделать, так как число элементов в W_i бесконечно, а число элементов, которые мы условились включать в I к i-му шагу, окажется конечным), и условившись не включать его в I. Чтобы I содержало не меньше i элементов, сделаем следующее: выберем числа $p_1, \ldots, p_i$, которые мы еще не условились не включать в I (такие будут, так как к i-му шагу мы условимся не включать в I лишь конечное множество чисел), и условимся включать $p_1, \ldots, p_i$ в I. Искомым множеством будет объединение возрастающей последовательности конечных множеств, i-й член которой содержит те числа, которые мы условились включать в I на i-м шаге.

2.17. Функция f либо тождественно равна 1, либо совпадает с одной из функций g_i, где

$$g_i(x)=\begin{cases}1 & \text{при} \quad x \leqslant i,\\ 0 & \text{при} \quad x > i.\end{cases}$$

Все эти функции вычислимы.

2.18. Да, является. Вычисляя e с все возрастающей точностью (например, с помощью известного ряда из обратных факториалов), мы рано или поздно убедимся в том, что $\frac{m}{n} < e$, или в том, что $\frac{m}{n} > e$. (Равенство $\frac{m}{n} = e$ невозможно, так как e иррационально.)

2.19. Да, ср. 2.18.

2.20. Достаточно рассмотреть случай иррационального x, так как в случае рационального x все три условия выполнены.

2.22. Множество всех действительных чисел несчетно, а множество всех вычислимых действительных чисел счетно: их не больше, чем задающих их алгоритмов.

3.1. Ср. лемму 6 (§ 3).

3.2. Очевидно следует из 3.1.

4.1. Формулу $\forall_ч x_n \alpha$ можно заменить на формулу $\forall x_n$ ($[x_n$ четно$] \to \alpha$).

4.2. Рассмотрите 8 возможностей для истинностных значений суждений α, β и γ.

4.4. Воспользуйтесь утверждениями задач 4.2 (формулы м), к), л)) и 4.3 (формула б)).

4.5. Ср. примеры 1, 3, 5 приложения Б.

4.6. См. приложение В.

4.7. Формулу $(x = n)$ можно заменить на эквивалентную, но не содержащую цифр. К примеру, $(x = 0)$ эквивалентно $(x + x = x)$, $(x = 1)$ эквивалентно формуле $(x \cdot x = x) \wedge \neg(x = 0)$ (осталось заменить $(x = 0)$ на описанную выше формулу), $(x = 2)$ — формуле $\exists y((y = 1) \wedge (x = y + y))$ и т. д.

4.8. Семейство всех арифметических множеств счетно, а семейство всех подмножеств $\mathbb{N}$ несчетно.

5.1. См. следствие 1 аксиомы протокола. Чтобы доказать а)$\to$б), заметим, что множество значений всюду определенной функции f равно области определения функции g:

$g(n) =$ (наименьшее k, для которого $f(k) = n$).

5.2. Ср. 2.13.

5.3. Это множество есть проекция множества

$$(\text{график } f)\cap(\mathbb{N}\times\{1981\}).$$

5.4. Если G — всюду определенная функция из $\mathbb{N}^2$ в $\mathbb{N}$, то функция g, определенная формулой

$$g(x)=G(x,x)+1,$$

не содержится среди функций G_n. Значит, G не является универсальной.

5.6. Если бы множество $M=\{x\,|\,\alpha(x)=1981\}$ было разрешимым, то функция β, определенная формулой

$$\beta(x)=\begin{cases}1981, & \text{если } x\notin M,\\ 0, & \text{если } x\in M,\end{cases}$$

была бы вычислимой всюду отличающейся от α функцией.

5.7. Пусть P — перечислимое неразрешимое подмножество $\mathbb{N}$. Множество $(P\times\{0\})\cup((\mathbb{N}\setminus P)\times\{1\})$ — искомое.

5.8. Пусть G — вычислимая функция из $\mathbb{N}^3$ в $\mathbb{N}$, универсальная для класса всех вычислимых функций из $\mathbb{N}^2$ в $\mathbb{N}$ в следующем смысле: среди функций G_n, определяемых формулой $G_n(x,y)=G(n,x,y)$, встречаются все вычислимые функции из $\mathbb{N}^2$ в $\mathbb{N}$. Рассмотрим функцию F из $\mathbb{N}^2$ в $\mathbb{N}$, определяемую формулой

$$F(k,x)=G(\xi(k),\eta(k),x),$$

где ξ и η — функции из доказательства леммы 5 (§ 3). Она и будет искомой.

5.9. Они являются проекциями множеств (график f) и (график $f)\cap(\mathbb{N}\times\mathbb{N}\times 1980)$.

5.10. Пусть f — вычислимая функция из $\mathbb{N}$ в $\mathbb{N}$ с неразрешимой областью определения. Положим

$$F(m,n)=\begin{cases}f(m), & \text{если } m=n,\\ \text{не определено}, & \text{если } m\neq n.\end{cases}$$

5.11. Пусть K — перечислимое неразрешимое множество. Положим $P=(K\times\{0\})\cup(\mathbb{N}\times\{1\})$.

5.12. Возьмем в качестве P область определения универсальной (для класса вычислимых функций из $\mathbb{N}$ в $\mathbb{N}$) вычислимой функции.

5.13. Если бы $Q = \{x \mid \langle x, x\rangle \notin P\}$ было перечислимым, то оно равнялось бы P_n при некотором n, а это невозможно, так как $n \in Q \leftrightarrow n \notin P_n$.

5.14. Если R — разрешимое подмножество $\mathbb{N}^2$, то множество S, определенное формулой $S = \{x \mid \langle x, x\rangle \notin S\}$, — разрешимое подмножество $\mathbb{N}$, отличное от всех сечений множества R.

5.15. Решение этой задачи можно прочесть на с. 141 упоминавшейся в предисловии книги Х. Роджерса или на с. 287 книги автора «Лекции о вычислимых функциях» (М.: Физматгиз, 1960, 492 с.).

5.16. Пусть $p(0), p(1), \ldots$ — перечисление перечислимого неразрешимого множества P. Тогда множество

$$R = \{(p(i)\text{-е простое число})^{i} \mid i \in \mathbb{N}\} \text{ — искомое.}$$

А.1. Если бы множество A было разрешимым, то оно было бы разрешимым множеством, отделяющим A от B.

А.2. В качестве множеств A, B и C можно взять множества $\{x \mid \alpha(x) = 0\}$, $\{x \mid \alpha(x) = 1\}$ и $\{x \mid \alpha(x) = 2\}$, где α — вычислимая функция, от которой ни одна вычислимая функция не может отличаться всюду.

А.3. Воспользуйтесь упражнением 2.12.

А.4. В качестве A и B можно взять неарифметические множества, дополняющие друг друга до $\mathbb{N}$.

Б.3. В качестве всюду определенного арифметического продолжения арифметической функции f можно взять функцию $\tilde{f}$, определенную формулой

$$\tilde{f}(n) = \begin{cases} f(n), & \text{если } f(n) \text{ определено,} \\ 0, & \text{если } f(n) \text{ не определено.} \end{cases}$$

Б.4. Если класс множеств содержит множества из примера 6 приложения Б и удовлетворяет утверждениям лемм Б.1 — Б.4, то он содержит множества, сопряженные с формулами вида $(t = s)$ и со всеми формулами, построенными из них (доказать индукцией по длине формулы), т. е. содержит все арифметические множества.

Б.5. Это утверждение надо доказывать индукцией по k. При $k = 0$ оно вытекает из того, что интересующее нас множество разрешимо. Переход от k к $k+1$ осуществляется следующим образом. Пусть B_k есть множество истинных суждений кванторной глубины

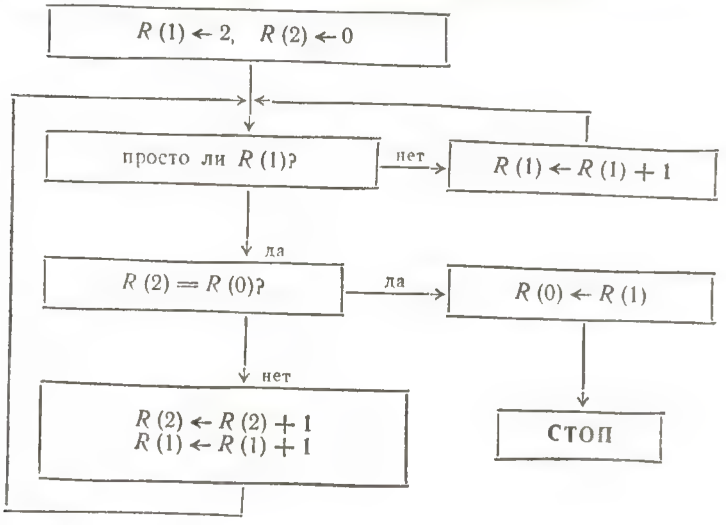
не больше k. Рассмотрим множества A_{k+1} и E_{k+1}, состоящие из всех истинных формул глубины не больше $k+1$, начинающихся с кванторов $\forall$ и $\exists$ соответственно. Используя арифметичность B_k, докажите арифметичность A_{k+1} и E_{k+1}. Затем докажите арифметичность B_{k+1}. Заметим, что с ростом k кванторная глубина формулы, с которой сопряжено B_k, возрастает. Как можно доказать, это обстоятельство неизбежно: при достаточно больших k множество B_k не сопряжено ни с какой формулой данной кванторной глубины.

Б.6. Используйте рассуждение, изложенное в конце приложения Б.

В.1. а) Вот требуемая программа:

1 $R(1) \leftarrow 0$
2 $R(2) \leftarrow 1$
3 $R(3) \leftarrow 2$
4 $R(4) \leftarrow 1$
5 **ЕСЛИ** $R(1) = R(0)$ **ТО ИДТИ К** 9 **ИНАЧЕ К** 6
6 $R(1) \leftarrow R(1) + R(4)$
7 $R(2) \leftarrow R(2) \cdot R(3)$
8 **ИДТИ К** 5
9 $R(0) \leftarrow R(2)$
10 **СТОП**

в) Общий замысел построения требуемой адресной программы может быть описан блок-схемой



Проверка простоты числа $R(1)$ реализуется, например, с помощью перебора всех чисел, меньших $R(1)$; для каждого из них проверяется делимость $R(1)$ на него.

д) Воспользуйтесь известным рядом для e (сумма обратных факториалов).

В.2. Финитную последовательность натуральных чисел можно закодировать одним числом. Поэтому работу адресной машины с бесконечным числом регистров можно моделировать на машине со 100 регистрами, записывая в одном из них (в виде кода) содержимое памяти моделируемой машины и используя остальные 99 для промежуточных вычислений, необходимых при моделировании (кодирования, декодирования и др.).

В.3. При моделировании, описанном в указании к упражнению В.2, нетрудно промоделировать также и косвенную адресацию.

В.4. Воспользоваться упражнением В.1 и арифметичностью адресно вычислимых функций.

В.5. Утверждение (для всех финитных v) α можно заменить на

$$\text{(для всех } v\text{)} \ \ ([v \text{ финитно}] \to \alpha),$$

где $[v$ финитно$]$ можно записать так:

$$\exists x_1 \forall x_2 (v(x_1 + x_2) = 0).$$

В.6. Имеет место эквивалентность:

(суждение с номером n истинно) $\leftrightarrow$ (существует функция, сопоставляющая всем суждениям арифметики одно из значений *И* и *Л*, обладающая указанными в определении истинности свойствами и сопоставляющая n-му суждению значение *И*).

В.7. Вычислимая функция, осуществляющая взаимно однозначное соответствие между $\mathbb{N}^2$ и $\mathbb{N}$, арифметична. Применяя ее, можно закодировать двуместные функции с помощью одноместных.

В.8. Проведите рассуждения, аналогичные примененным при доказательстве теоремы Тарского. Второе утверждение задачи аналогично утверждению упражнения В.6.

В.9. Пусть все адресные программы закодированы натуральными числами. Докажите, что при естественном выборе такого кодирования функция F из $\mathbb{N}^4$ в $\mathbb{N}$,

определенная формулой $F(n, x, y, k) =$ (содержимое y-го регистра после k шагов применения адресной программы с кодом n к исходному данному x), адресно вычислима. (Вычислимость этой функции очевидна.)

В.10. См. указание к упражнению В.9.

Г.1. Это исчисление разрешимо. Разрешающий алгоритм таков. Пусть даны слова P и Q. Чтобы определить, эквивалентны ли они, надо заменить в них группы из повторяющихся букв a на одиночные буквы a, а также сделать то же самое с группами из букв b. (Например, слово *aaababbaa* превратится при этом в *ababa*.) Если после применения этой операции к словам P и Q получится одно и то же слово, то P и Q эквивалентны друг другу; если нет, то не эквивалентны.

Г.2. Пусть исчисление имеет вид

$$a^{n_1} \leftrightarrow a^{m_1},$$
$$a^{n_2} \leftrightarrow a^{m_2},$$
$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot$$
$$a^{n_k} \leftrightarrow a^{m_k},$$

при всех i выполнено $m_i \neq n_i$ и через l_i обозначено $|m_i - n_i|$, p — наименьшее число среди m_i и n_i. Тогда все слова длины меньше p не эквивалентны друг другу и остальным словам (ибо к ним вообще нельзя применить подстановку), а слова длин m и n $(m, n \geqslant p)$ эквивалентны друг другу тогда и только тогда, когда разность $m - n$ делится на НОД$(l_1, \ldots, l_k)$.

Г.3. Слово *babaa* преобразуется в *baaba* (результативная остановка); слово *abaab* в процессе преобразования переходит в слово *bbabab* и дальнейшее применение алгоритма невозможно (безрезультатная остановка); слово *baaba* испытывает такие преобразования:

baaba → *abaaba* → *baabab* → *abababa* →
→ *bababab* → *babababa* → ...

Этот процесс продолжается до бесконечности, поскольку слово

ba ... ba (n раз) преобразуется в слово
aba ... aba (n раз), а затем в слово
ba ... ba ($2n$ раз).

Г.4. Всякое слово этого исчисления эквивалентно одному из слов a, ac, acc, $accc$, ,c, cc, ccc (эти 8 слов, пятое из которых пусто, мы будем называть приведенными). В самом деле, с помощью подстановки $b \leftrightarrow acc$ можно устранить все вхождения буквы b, затем с помощью подстановки $ca \leftrightarrow accc$ добиться того, чтобы все буквы a были левее всех букв c. Применяя теперь подстановки $aa \leftrightarrow$ и $cccc \leftrightarrow$, мы можем добиться, чтобы число вхождений буквы a не превосходило 1, а число вхождений буквы c не превосходило 3.

Докажем, что различные приведенные слова не эквивалентны друг другу. В самом деле, сопоставим каждому слову некоторое преобразование квадрата в себя (если угодно, некоторую перестановку четырехэлементного множества вершин квадрата). Именно, слову c сопоставим поворот квадрата на 90° вокруг центра, слову a — осевую симметрию относительно оси, параллельной одной из сторон квадрата, слову b — осевую симметрию относительно оси, параллельной другой стороне квадрата. Слову, получающемуся при приписывании друг к другу слов P и Q, сопоставим композицию соответствующих преобразований (сначала P, затем Q). Нетрудно проверить, что эквивалентным словам соответствуют одинаковые преобразования, а различным приведенным словам — разные.

Разрешающий алгоритм таков: чтобы узнать, эквивалентны ли слова P и Q, надо заменить их на приведенные эквиваленты и сравнить эти эквиваленты. Если они равны, то слова P и Q эквивалентны; если не равны, то не эквивалентны.

Владимир Андреевич Успенский

ТЕОРЕМА ГЕДЕЛЯ О НЕПОЛНОТЕ

(Серия: «Популярные лекции по математике»)

Редактор *В. В. Донченко*
Техн. редактор *Н. В. Вершинина*
Корректоры *О. А. Сигал, М. Л. Медведская*

ИБ № 11797

Сдано в набор 08.06.81. Подписано к печати 08.01.82. Формат $84 \times 108^1/_{32}$, бумага тип. № 3. Литературная гарнитура. Высокая печать. Условн. печ. л. 5,88. Уч.-изд. л. 5,81. Тираж 100 000 экз. Заказ № 1171. Цена 15 коп.

Издательство «Наука»
Главная редакция
физико-математической литературы
117071, Москва, В-71, Ленинский проспект, 15

Ленинградская типография № 2 головное предприятие ордена Трудового Красного Знамени Ленинградского объединения «Техническая книга» им. Евгении Соколовой Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 198052, г. Ленинград, Л-52, Измайловский проспект, 29.

15 коп.

ПОПУЛЯРНЫЕ ЛЕКЦИИ ПО МАТЕМАТИКЕ